

---

# CHAPTER 1

---

## INTRODUCTION

---

In 1978, a series of unofficial exchange visits between US nuclear weapons experts and their People's Republic of China (PRC) counterparts began. The PRC officials made a serious concentrated effort to cultivate close relationships with certain US experts. Over the subsequent 23 years, as a result of this exchange, the PRC made major strides in the development of nuclear weapons, including the neutron bomb.

Beginning in 1998, US media sources began reporting about ongoing investigations of four cases of suspected Chinese espionage against the United States dating back to the 1980s. The most serious case involved China's alleged acquisition of key information about our nation's most advanced miniaturized US nuclear warhead, the W-88, as well as serious security breaches at the Department of Energy's (DOE) Los Alamos Laboratory between 1984 and 1988.

Early in 1998, Congressional focus turned to US satellite exports to China. A US Department of Defense classified report concluded that scientists from Hughes and Loral Space and Communications, involved in studying the 1996 crash of a Chinese rocket launching a Loral satellite, provided scientific expertise to China that notably improved the reliability of China's missile launch abilities.

After this information was published in the US media, a special House Select Committee and a number of Senate committees investigated US technology transfer policy with respect to China. The result was the release of the Report of the Select Committee on U.S. National Security and Military/Commercial Concerns With the People's Republic of China (the Cox Report). The report dealt, among other things, with the possible compromise of highly classified information on DOE's nuclear weapons laboratories.

After the release of the Cox Report, President William Clinton requested the President's Foreign Intelligence Advisory Board (PFIAB), chaired by former Senator Walter Rudman, to review the security threat at DOE's nuclear weapons laboratories and the measures taken to address that threat. In June 1999, the PFIAB presented its report to the President. The report found that DOE "is a dysfunctional bureaucracy that has proven it is incapable of reforming itself."

In 1999, the press reported about an investigation by the FBI against a Taiwan-born Chinese American scientist, Wen Ho Lee, who downloaded critical nuclear weapons codes, called legacy codes, from a classified computer system at Los Alamos to an unclassified system accessible by anyone with the proper password. Suspected of espionage, Wen Ho Lee was charged with only one count of mishandling national security information to which he pled guilty and sentenced to time served. The FBI came under heavy criticism that it mishandled the investigation and exaggerated the case against Lee.

Congressional concern over security at the nuclear weapons laboratories increased again in June 2000 when it was discovered that computer hard drives containing nuclear weapons information disappeared at Los Alamos. The drives later turned up, and a FBI investigation of the missing failed to determine who took them.

A major crisis between China and the United States occurred when a US Navy EP-3 reconnaissance aircraft, conducting a routine and solo reconnaissance mission approximately 50 to 60 miles off the Chinese coast, collided with a Chinese jet fighter on 1 April 2001. The Chinese fighter crashed, and the pilot died. The US Navy plane made an emergency landing at a military base on China's Hainan Island. The Chinese held the Navy

---

crew for 11 days and released them only when the US Ambassador delivered a letter of regret over the intrusion of China's airspace and landing without verbal clearance from the Chinese.

In 1999, the American press began to publish articles that stated the Chinese Government was arresting prominent activists and handing out harsh jail sentences for reasonable civil liberties. On 15 August 1999 two independent researchers, one of whom was an American, were arrested for conducting interviews about a pending World Bank project. During an interrogation by Chinese security officials, the American was seriously injured when he jumped out of a third story window.

In early 2000, Chinese authorities initiated a major crackdown against overseas Chinese visitors, some of whom had US connections. They arrested eight American citizens or permanent residents of the United States. The arrests clouded bilateral relations between the United States and China and were raised at the highest political level. Several were subsequently tried, convicted, and allowed to leave China.

Chinese intelligence, like those of other countries in the post-Cold War era, has increasingly focused on economic, industrial, commercial, and technological information. There have been reports of Chinese companies in the United States being connected to China's military industrial complex through which American technologies are allegedly being transferred back to China. In addition, corporate espionage and illegal transfer of American technology will increase as the United States and China expands their relationship both politically and commercially.

---

## **Huang** Dao Pei

The FBI arrested Huang Dao Pei, a Chinese-born naturalized US citizen living in Piscataway, New Jersey, on 28 July 1998 on charges he tried to steal trade secrets for a hepatitis C monitoring kit he hoped to sell in China. Huang, a former scientist who worked at Roche Diagnostics from 1992 to 1995, allegedly tried to buy information from a scientist who worked for Roche. The scientist was cooperating with the FBI.

According to court papers, Huang telephoned the cooperating scientist on two occasions asking for specific documents that would help him duplicate parts of the kit. Huang promised to pay the scientist for the risk involved in obtaining the documents. He told the scientist he needed the information so his firm, LCC Enterprises, could develop a similar kit and sell it in China.

As reported in the open press, the FBI declined to say whether Huang was working for the Chinese, but it was noted that China is among the most aggressive countries going after US trade secrets. A Roche representative stated that, if a competitor were to obtain the information sought by Huang, it could avoid spending the millions of dollars and years that Roche spent developing the product.

---

## **Peter** H. Lee—Update<sup>1</sup>

On 26 March 1998, Dr. Peter S. Lee, the nuclear physicist convicted of two felony counts including passing classified national defense information to PRC representatives, was sentenced to spend one year in a community corrections facility. In addition to the one-year term, he was ordered to serve three years of probation, perform 3,000 hours of community service, and pay \$20,000 in fines.

In a case apparently involving empathy instead of greed, Lee admitted under a plea bargain agreement on 7 December 1997, that he passed classified defense secrets to the Chinese Government in 1985 while working as a research physicist at Los Alamos National Laboratory. Lee, a naturalized US citizen who was born in Taiwan, was working on classified projects relating to the use of lasers to simulate nuclear detonations. The information was declassified in the early 1990s. He was fired by TRW on the same day he pleaded guilty.

Lee passed the classified information in 1985 while he was doing research at the Los Alamos National Laboratory in New Mexico. Lee had traveled to China where he was asked by a Chinese scientist to discuss the construction of hohlraums, a diagnostic device used in conjunction with lasers to create microscopic nuclear detonations. The day after he initially revealed the classified information, Lee gave a lecture to about 30 Chinese nuclear scientists in which he again gave away secret restricted data regarding the manufacture and use of hohlraums. Lee told the FBI that he disclosed the information because he wanted to help his Chinese counterparts, and he wanted to enhance his reputation there.

The second charge against Lee concerns disclosures he failed to make in 1997 while he was working on classified research projects for TRW. Before he traveled to China on vacation, Lee was required to fill out a security form in which he stated that he would not be giving lectures on his work during his trip. Upon his return, he had to fill out a second form in which he confirmed that he did not give any lectures of a technical nature.

---

However, as Lee later confessed to the FBI, he lied on both forms because he intended to and did, in fact, deliver lectures to Chinese scientists that discussed his work at TRW.

---

### Endnote

<sup>1</sup> For previous information on Peter Lee, see *Counterintelligence Reader*, Volume III, p. 410.

---

## The Cox Report

*(Editor's Note: This edited version of the report written by the Select Committee on U.S. National Security and Military/Commercial Concerns with The People's Republic of China [referred to as the Cox Committee] is printed verbatim. This edited version of the Committee's report [known as the Cox Report] concentrates on China's collection methodologies in obtaining US technology and the US investigation of those methodologies.)*

It is extremely difficult to meet the challenge of the PRC's technology acquisition efforts in the United States with traditional counterintelligence techniques that were applied to the Soviet Union. Whereas Russians were severely restricted in their ability to enter the United States or to travel within it, visiting PRC nationals, most of whom, come to pursue lawful objectives, are not so restricted. Yet the PRC employs all types of people, organizations, and collection operations to acquire sensitive technology: threats to national security can come from PRC scientists, students, business people, or bureaucrats, in addition to professional civilian and military intelligence operations.

The PRC is striving to acquire advanced technology of any sort, whether for military or civilian purposes, as part of its program to improve its entire economic infrastructure.<sup>1</sup> This broad targeting permits the effective use of a wide variety of means to access technology. In addition, the PRC's diffuse and multi-pronged technology-acquisition effort presents unique difficulties for US intelligence and law enforcement agencies, because the same set of mechanisms and organizations used to collect technology in general can be used, and are used to collect military technology.

In light of the number of interactions taking place between PRC and US citizens and organizations over the last decade as trade and other forms of cooperation have bloomed, the opportunities for the PRC to attempt to acquire information and technology, including sensitive national security secrets, are immense. Moreover, the PRC often

---

does not rely on centralized control or coordination in its technology acquisition efforts, rendering traditional law enforcement, intelligence, and counterintelligence approaches inadequate. While it is certainly true that not all of the PRC's technology acquisition efforts are a threat to US national security, that very fact makes it quite a challenge to identify those that are.

The PRC's blending of intelligence and non-intelligence assets and reliance on different collection methods presents challenges to US agencies in meeting the threat. In short, as James Lilley, former US Ambassador to the PRC says, US agencies are "going nuts" trying to find MSS and MID links to the PRC's military science and technology collection, when such links are buried beneath layers of bureaucracy or do not exist at all.<sup>2</sup>

### **Commercial and intelligence operations: PRC acquisition of US technology**

The State Council controls the PRC's military-industrial organizations through the State Commission of Science, Technology and Industry for National Defense (COSTIND). Created in 1982, COSTIND was originally intended to eliminate conflicts between the military research and development sector and the military production sector by combining them under one organization. Soon its role broadened to include the integration of civilian research, development, and production efforts into the military.

COSTIND presides over a vast, interlocking network of institutions dedicated to the specification, appraisal, and application of advanced technologies to the PRC's military aims. The largest of these institutions are styled as corporations, notwithstanding that they are directly in service of the Chinese Communist Party (CCP), the PLA, and the State. They are:

- China Aerospace Corporation (CASC)
- China National Nuclear Corporation (CNNC)
- China North Industries Group (NORINCO)

- Aviation Industries Corporation of China (AVIC)
- China State Shipbuilding Corporation (CSSC)

Until 1998, COSTIND was controlled directly by both the Central Military Commission and the State Council. In March 1998, COSTIND was "civilianized" and now reports solely to the State Council. A new entity, the General Armament Department (GAD), was simultaneously created under the CMC to assume responsibility for weapons system management and research and development.

### **The 863 and Super-863 Programs: Importing Technologies for Military Use**

In 1986, "Paramount Leader" Deng Xiaoping<sup>3</sup> adopted a major initiative, the so-called 863 Program, to accelerate the acquisition and development of science and technology in the PRC.<sup>4</sup> Deng directed 200 scientists to develop science and technology goals. The PRC claims that the 863 Program produced nearly 1,500 research achievements by 1996 and was supported by nearly 30,000 scientific and technical personnel who worked to advance the PRC's "economy and . . . national defense construction."<sup>5</sup>

The most senior engineers behind the 863 Program were involved in strategic military programs such as space tracking, nuclear energy, and satellites.<sup>6</sup> Placed under COSTIND's management, the 863 Program aimed to narrow the gap between the PRC and the West by the year 2000 in key science and technology sectors, including the military technology areas of:

- Astronautics
- Information technology
- Laser technology
- Automation technology
- Energy technology
- New materials

The 863 Program was given a budget split between military and civilian projects, and focuses on both

---

military and civilian science and technology. The following are key areas of military concern:

- **Biological Warfare:** The 863 Program includes a recently unveiled plan for gene research that could have biological warfare applications.
- **Space Technology:** Recent PRC planning has focused on the development of satellites with remote sensing capabilities, which could be used for military reconnaissance, as well as space launch vehicles.
- **Military Information Technology:** The 863 Program includes the development of intelligent computers, optoelectronics, and image processing for weather forecasting; and the production of submicron integrated circuits on 8-inch silicon wafers. These programs could lead to the development of military communications systems; command, control, communications, and intelligence systems; and advances in military software development.
- **Laser Weapons:** The 863 Program includes the development of pulse-power techniques, plasma technology, and laser spectroscopy, all of which are useful in the development of laser weapons.
- **Automation Technology:** This area of the 863 Program, which includes the development of computer-integrated manufacturing systems and robotics for increased production capability, is focused in the areas of electronics, machinery, space, chemistry, and telecommunications, and could standardize and improve the PRC's military production.
- **Nuclear Weapons:** Qinghua University Nuclear Research Institute has claimed success in the development of high-temperature, gas-cooled reactors, projects that could aid in the development of nuclear weapons.
- **Exotic Materials:** The 863 Program areas include optoelectronic information materials, structural materials, special function materials,

composites, rare-earth metals, new energy compound materials, and high-capacity engineering plastics. These projects could advance the PRC's development of materials, such as composites, for military aircraft and other weapons.

In 1996, the PRC announced the "Super 863 Program" as a follow-on to the 863 Program, planning technology development through 2010. The "Super 863 Program" continues the research agenda of the 863 Program, which apparently failed to meet the CCP's expectations.

The Super 863 Program calls for continued acquisition and development of technology in a number of areas of military concern, including machine tools, electronics, petrochemicals, electronic information, bioengineering, exotic materials, nuclear research, aviation, space, and marine technology.

COSTIND and the Ministry of Science and Technology jointly manage the Super 863 Program. The Ministry of Science and Technology focuses on biotechnology, information technology, automation, nuclear research, and exotic materials, while COSTIND oversees the laser and space technology fields.<sup>7</sup>

COSTIND is attempting to monitor foreign technologies, including all those imported into the PRC through joint ventures with the United States and other Western countries. These efforts are evidence that the PRC engages in extensive oversight of imported dual-use technology. The PRC is also working to translate foreign technical data, analyze it, and assimilate it for PLA military programs. The Select Committee has concluded that these efforts have targeted the US Government and other entities.

If successful, the 863 Programs will increase the PRC's ability to understand, assimilate, and transfer imported civil technologies to military programs. Moreover, Super 863 Program initiatives increasingly focus on the development



---

of technologies for military applications. PRC program managers are now emphasizing projects that will attract US researchers.

Since the early 1990s, the PRC has been increasingly focused on acquiring US and foreign technology and equipment, including particularly dual-use technologies that can be integrated into the PRC's military and industrial bases.

### **The PRC's Use of Intelligence Services To Acquire US Military Technology**

The primary professional PRC intelligence services involved in technology acquisition are the Ministry of State Security (MSS) and the PLA General Staff's Military Intelligence Department (MID).

In addition to and separate from these services, the PRC maintains a growing non-professional technology-collection effort by other PRC Government-controlled interests, such as research institutes and PRC military-industrial companies. Many of the most egregious losses of US technology have resulted not from professional operations under the control or direction of the MSS or MID, but as part of commercial, scientific, and academic interactions between the United States and the PRC.

Professional intelligence collectors, from the MSS and MID, account for a relatively small share of the PRC's foreign science and technology collection. Various non-professionals, including PRC students, scientists, researchers, and other visitors to the West, gather the bulk of such information. These individuals sometimes are working at the behest of the MSS or MID, but often represent other PRC-controlled research organizations - scientific bureaus, commissions, research institutes, and enterprises.

Those unfamiliar with the PRC's intelligence practices often conclude that, because intelligence services conduct clandestine operations, all clandestine operations are directed by intelligence agencies. In the case of the PRC, this is not always

the rule. Much of the PRC's intelligence collection is independent of MSS direction. For example, a government scientific institute may work on its own to acquire information.

Minister Xu Yongyue, a member of the CCP Central Committee, heads the MSS. The MSS reports to Premier Zhu Rongji and the State Council, and its activities are ultimately overseen by the CCP Political Science and Law Commission. It is a usual practice for senior members of the CCP's top leadership to be interested in the planning of PRC military acquisitions.

The MSS conducts science and technology collection as part of the PRC's overall efforts in this area. These MSS efforts most often support the goals of specific PRC technology acquisition programs, but the MSS will take advantage of any opportunity to acquire military technology that presents itself.

The MSS relies on a network of non-professional individuals and organizations acting outside the direct control of the intelligence services, including scientific delegations and PRC nationals working abroad, to collect the vast majority of the information it seeks.

The PLA's MID, also known as the Second Department of the PLA General Staff, is responsible for military intelligence. PLA General Ji Shengde, the son of a former PRC Foreign Minister, currently runs it. One of the MID's substantial roles is military-related science and technology collection.

### **The 'Princelings'**

Unlike the Soviet Union, where nepotism in the Communist Party was rare, ruling in the PRC is a family business. Relatives of the founders of the Chinese Communist Party rise quickly through the ranks and assume powerful positions in the CCP, the State, the PLA, or the business sector. These leaders, who owe their positions more to family

---

connections than to their own merit, are widely known as “princelings.”<sup>8</sup>

Political, military, and business leaders in the PRC exercise considerable influence within their respective hierarchies. With the exception of those who make their way to the uppermost levels of the CCP or State bureaucracies, however, their authority, power, and influence extend only to those below them within that hierarchy. They have little ability to influence either the leaders above them within their own hierarchy or the leaders in other hierarchies.<sup>9</sup>

Princelings operate outside these structures. Because of their family ties and personal connections to other CCP, PLA, and State officials, they are able to “cross the lines” and accomplish things that might not otherwise be possible.<sup>10</sup>

The Cox Committee identified two as most notable princelings, Wang Jun and Liu Chaoying, which the Committee said had been directly involved in illegal activities in the United States.

Wang Jun is the son of the late PRC President Wang Zhen. At the time, Wang simultaneously held two powerful positions in the PRC. He was Chairman of the China International Trade and Investment Company (CITIC), the most powerful and visible corporate conglomerate in the PRC. He was also the President of Polytechnologies Corporation, an arms-trading company and the largest and most profitable of the corporate structures owned by the PLA. Wang’s position gave him considerable clout in the business, political, and military hierarchies in the PRC.<sup>11</sup>

Wang was publicly known in the United States for his role in the 1996 campaign finance scandal and for Polytechnologies’ indictment stemming from its 1996 attempt to smuggle 2,000 Chinese AK-47 assault rifles into the United States. He attended a White House “coffee” with President Clinton in February 1996 and met with Commerce Secretary Ronald Brown the following day. He was also connected to over \$600,000 in illegal campaign

contributions made by Charlie Trie to the US Democratic National Committee (DNC).<sup>12</sup>

Liu Chaoying is the daughter of former CCP Central Military Commission Vice-Chairman and Politburo Standing Committee member General Liu Huaqing, who has used numerous US companies for sensitive technology acquisitions. General Liu has been described as the PLA’s preeminent policymaker on military R&D, technology acquisition, and equipment modernization as well as the most powerful military leader in the PRC. His daughter was a Lieutenant Colonel in the PLA and has held several key and instrumental positions in the PRC’s military industry, which is involved in numerous arms transactions and international smuggling operations.<sup>13</sup> On two occasions, she has entered the United States illegally and under a false identity.

Col. Liu Chaoying was then a Vice-President of China Aerospace International Holdings, a firm specializing in foreign technology and military sales.<sup>14</sup> It is the Hong Kong subsidiary of China Aerospace Corporation, the organization that manages the PRC’s missile and space industry. Both organizations benefit from the export of missile or satellite-related technologies and components from the United States, as does China Great Wall Industry Corporation, Col. Liu’s former employer and a subsidiary of China Aerospace Corporation, which provides commercial space launch services to American satellite manufacturers.

China Aerospace Corporation is also a substantial shareholder in both the Apstar and APMT projects to import US satellites to the PRC for launch by China Great Wall Industry Corporation.<sup>15</sup>

A Chinese-American, Johnny Chung, during the course of plea negotiations, disclosed that during a trip to Hong Kong in the summer of 1996, he met with Col. Liu and the head of the MID, Gen. Ji Shengde. According to Chung, he received \$300,000 from Col. Liu and Gen. Ji as a result of this meeting. The FBI confirmed the deposit into



---

Chung's account from Hong Kong and that the PLA officials likely served as the conduit for the money.

The Cox Committee determined that Col. Liu's payment to Johnny Chung was an attempt to better position her in the United States to acquire computer, missile, and satellite technologies. The purpose of Col. Liu's contacts was apparently to establish reputable ties and financing for her acquisition of technology such as telecommunications and aircraft parts.<sup>16</sup>

Within one month after meeting with Col. Liu in Hong Kong, Chung formed Marswell Investment, Inc., possibly capitalizing the new company with some of the \$300,000 he had received from Col. Liu and Gen. Ji.<sup>17</sup> Col. Liu was designated as president of the company, which was based in Torrance, California. The company is located in southern California, in the same city where China Great Wall Industry Corporation also maintains its US subsidiary.

Col. Liu made two trips to the United States, one in July 1996 and one in August 1996, apparently seeking to expand her political and commercial contacts. During Col. Liu's July trip, Chung arranged for her to attend a DNC fundraiser where she met President Clinton and executives involved in the import-export business.<sup>18</sup> Shortly afterwards, Chung also arranged for her to meet with the Executive Vice President of the Federal Reserve Bank of New York.<sup>19</sup>

Liu's August 1996 trip to the United States came at the invitation of Chung, who had told her that he had contacted Boeing and McDonnell Douglas regarding her interest in purchasing aircraft parts.<sup>20</sup>

That same month, Col. Liu traveled to Washington, D.C., where Chung had contacts arrange for her to meet with representatives of the Securities and Exchange Commission to discuss listing a PRC company on US stock exchanges.<sup>21</sup> Soon after the meeting, when Chung and Liu's alleged involvement in the campaign finance scandal

became the subject of media reports, Col. Liu left the United States. Marswell remains dormant.<sup>22</sup>

Princelings such as Wang and Liu present a unique technology transfer threat because their multiple connections enable them to move freely around the world and among the different bureaucracies in the PRC. They are therefore in a position to pull together the many resources necessary to carry out sophisticated and coordinated technology acquisition efforts.<sup>23</sup>

### **Acquisition of Military Technology from the United States**

The PRC has stolen military technology from the United States, but until recently, the United States has lawfully transferred little to the PLA. This has been due, in part, to the sanctions imposed by the United States in response to both the 1989 Tiananmen Square massacre and to the PRC's 1993 transfer of missile technology to Pakistan.

During the Cold War, the United States assisted the PRC in avionics modernization of its jet fighters under the US Peace Pearl program.<sup>24</sup>

After the relatively "cool" period in US-PRC relations in the early 1990s, the trend since 1992 has been towards liberalization of dual-use technology transfers to the PRC.<sup>25</sup> Recent legal transfers include the sale of approximately 40 gas turbine jet engines, the sale of high performance computers, and licensed co-production of helicopters.

Nonetheless, the list of military-related technologies legally transferred to the PRC directly from the United States remains relatively small.

Illegal transfers of US technology from the US to the PRC, however, have been significant. Significant transfers of US military technology have also taken place in the mid-1990s through the re-export by Israel of advanced technology transferred to it by the United States, including

---

avionics and missile guidance useful for the PLA's F-10 fighter. Congress and several Executive agencies have also investigated allegations that Israel has provided US-origin cruise, air-to-air, and ground-to-air missile technology to the PRC.<sup>26</sup>

### **Joint Ventures with US Companies**

The vast majority of commercial business activity between the United States and the PRC does not present a threat to national security, but additional scrutiny, discipline, and an awareness of risks are necessary with respect to joint ventures with the PRC where the potential exists for the transfer of militarily-sensitive US technology.

The US 1997 National Science and Technology Strategy stated that: "Sales and contracts with foreign buyers imposing conditions leading to technology transfer, joint ventures with foreign partners involving technology sharing and next generation development, and foreign investments in US industry create technology transfer opportunities that may raise either economic or national security concerns."<sup>27</sup>

The behavior of the PRC Government and PRC-controlled businesses in dealing with US companies involved with militarily sensitive technology confirms that these concerns are valid and growing. The growing number of joint ventures that call for technology transfers between the PRC and US firms can be expected to provide the PRC with continued access to dual-use technologies for military and commercial advantage.

Technology transfer requirements in joint ventures often take the form of side agreements (sometimes referred to as offset agreements) requiring both that the US firm transfer technology to the PRC partner, and that all transferred technology will eventually become the property of the PRC partner.<sup>28</sup>

Although many countries require technology transfers when they do business with US firms, no country makes such demands across as wide a variety of industries as the PRC does.<sup>29</sup> Despite the

PRC's rapid economic liberalization since 1978, it continues to implement its explicitly designed goals and policies to restrict and manage foreign investment so as to bolster the PRC's military and commercial industries through acquisition of technology.<sup>30</sup>

The Communist Party has long believed that forcing technology from foreign firms is not only critical to the PRC, but also is a cost that foreign firms will bear in order to obtain PRC market entry.

In the past, the PRC has favored joint ventures with US high-technology companies for several reasons:

- The US excels in many areas of technology that are of special interest to the PLA and to PRC-controlled firms
- Many PRC scientists were educated in the United States and retain valuable contacts in the US research and business community who can be exploited for technology transfer
- Many other countries are more reluctant than the United States to give up technology<sup>31</sup>

The PRC has dedicated increasing resources to identifying US high-technology firms as likely targets for joint venture overtures. Science and technology representatives in PRC embassies abroad are used to assist in this targeting of technology, and to encourage collaboration with US firms for this purpose.

Unless they are briefed by the FBI pursuant to its National Security Threat List program, US companies are unaware of the extent of the PRC's espionage directed against US technology, and thus—at least from the US national security standpoint—are generally unprepared for the reality of doing business in the PRC. They lack knowledge of the interconnection between the CCP, the PLA, the State, and the PRC-controlled companies with which they deal directly in the negotiating process.<sup>32</sup>

The US General Accounting Office (GAO) has found that US businesses have significant concerns about arbitrary licensing requirements in the PRC that often call for increased technology transfer. The GAO has also found that transparency was the most frequent concern reported by US companies.<sup>33</sup> Because of the lack of transparency in the PRC's laws, rules, and regulations that govern business alliances, and the dearth of accessible, understandable sources of regulatory information, US businesses are often subjected to technology transfer requirements that are not in writing, or are not maintained in the field, or are contained in "secret" rules that only insiders know about.<sup>34</sup>

The PRC's massive potential consumer market is the key factor behind the willingness of some US businesses to risk and tolerate technology transfers. Some of these transfers could impair US national security, as in the cases of Loral and Hughes. The obvious potential of the PRC market has increasingly enabled the PRC to place technology-transfer demands on its US trading partners.

US businesses believe that they must be in the PRC, lest a competitor get a foothold first.<sup>35</sup> In fact, many US high-technology firms believe it is more important to establish this foothold than to make profits immediately or gain any more than limited access to the PRC market.<sup>36</sup> Some of the PRC's trading partners have focused on increased technology transfers to raise the attractiveness of their bids.

In addition to traditional types of technology transfer, many US high-technology investments in the PRC include agreements establishing joint research and development centers or projects. This type of agreement represents a new trend in US investment in the PRC and is a potentially significant development.<sup>37</sup>

US companies involved in joint ventures may be willing to transfer technology because they believe that the only risk is a business one - that is, that the transfers may eventually hurt them in terms of market share or competition.<sup>38</sup> These businesses may be unaware that technologies transferred to a

PRC partner will likely be shared within the PRC's industrial networks and with the PLA, or that joint ventures may be used in some instances as cover to acquire critical technology for the military.

COSTIND, which controls the PRC's military-industrial organizations, likely attempts to monitor technologies through joint ventures. In addition, US businesses may be unaware that joint-venture operations are also vulnerable to penetration by official PRC intelligence agencies, such as the MSS.

In one 1990s case reviewed by the Cox Committee, a US high-technology company and its PRC partner used a joint venture to avoid US export control laws and make a lucrative sale of controlled equipment to the PRC. Following the denial of an export license, the US company attempted to form a joint venture to which the technology would be transferred. The joint venture was controlled by a PRC entity included on the US Commerce Department's Entity List, which means it presents an unacceptable risk of diversion to the development of weapons of mass destruction.

## **Acquisition and Exploitation of Dual-Use Technologies**

The acquisition of advanced dual-use technology represents yet another method by which the PRC obtains advanced technology for military modernization from the United States. The PRC's military modernization drive includes a policy to acquire dual-use technologies. The PRC seeks civil technology in part in the hope of being able to adapt the technology to military applications. Some analysts refer this to as "spinning on."<sup>39</sup>

A strategy developed by the PRC in 1995 called for the acquisition of dual-use technologies with civil and military applications, and the transfer of R&D achievements in civil technology to the research and production of weapons.

The PRC collects military-related science and technology information from openly available

---

US and Western sources and military researchers. This accelerates the PLA's military technology development by permitting it to follow proven development options already undertaken by US and Western scientists.

PRC procurement agents have approached US firms to gain an understanding of the uses of available technology, and to evaluate the PRC's ability to purchase dual-use technology under the guise of civil programs and within the constraints of US export controls. Additionally, the PRC has attempted to acquire information from the US and other countries about the design and manufacturing of military helicopters.<sup>40</sup> The PRC could use this approach to acquire chemical and biological weapons technology.

The key organizations in the PRC's drive to acquire dual-use technology include:

- COSTIND acquires dual-use technology for PRC institutes and manufacturers by assuring foreign suppliers that the technology will be used for civil production. COSTIND uses overseas companies to target US firms for acquisition of dual-use technology for the military.
- The Ministry of Electronics Industry (MEI)<sup>41</sup> is responsible for developing the PRC's military electronics industry. Among other things, the Ministry approves and prioritizes research and development and the importation of electronics technologies that can be used to speed up the PRC's indigenous production capabilities.
- The Ministry of Post and Telecommunications (MPT) is acquiring asynchronous transfer mode switches that could be used for military purposes by the PLA.<sup>42</sup>
- PLA-operated import-export companies, which also import dual-use technologies for military modernization. Polytechnologies, a company attached to the General Staff Department of the PLA, plays a major role in this effort, especially in negotiating foreign weapons purchases.<sup>43</sup>
- AVIC, and its subsidiary, China National Aero-Technology Import-Export Corporation (CATIC), which have sent visitors to US firms to discuss manufacturing agreements for commercial systems that could be used to produce military aircraft for the PLA. AVIC is one of five PRC state-owned conglomerates that operate as "commercial businesses" under the direct control of the State Council and COSTIND.

Several incidents highlight CATIC's direct role in the acquisition of controlled US technology. One clear example was CATIC's role as the lead PRC representative in the 1994 purchase of advanced machine tools from McDonnell Douglas.

Another possible example of the PRC's exploitation of civilian end-use as a means of obtaining controlled technology was CATIC's 1983 purchase of two US-origin CFM-56 jet engines on the pretext that they would be used to re-engine commercial aircraft. Although the CFM-56 is a commercial engine, its core section is the same as the core of the General Electric F-101 engine that is used in the US B-1 bomber. Because of this, restrictions were placed on the export license. However, the PRC may have exploited the technology of the CFM-56. When the US Government subsequently requested access to the engines, the PRC claimed they had been destroyed in a fire.

CATIC has, on several occasions, misrepresented the proposed uses of militarily useful US technology. The Clinton administration determined that the specific facts in these cases may not be publicly disclosed without affecting national security.

In 1996, AVIC, CATIC's parent company, attempted to use a Canadian intermediary to hire former Pratt & Whitney engineers in the United States to assist in the development of an indigenous PRC jet engine. AVIC's initial approach was under the guise of a civilian project, and the US engineers were not told they would be working on a military engine for the PRC's newest fighter jet until

---

negotiations had progressed substantially. The US engineers pulled out when they were told what they would be asked to do.<sup>44</sup>

The degree of diversion to military programs by the PRC of commercially acquired technologies is unclear, since the PRC's parallel civil-military industrial complex<sup>45</sup> often blurs the true end-use of technology that is acquired. As a result, there may be more use of US dual-use technology for military production than these examples suggest.

## Front Companies

Another method by which the PRC acquires technology is through the use of front companies. The term "front company" has been used in a variety of ways in public reports and academic studies in different contexts, and can include:

- US subsidiaries of PRC military-industrial corporations in the PRC
- US subsidiaries of PLA-owned-and-operated corporations
- Corporations set up by PRC nationals overseas to conduct technology acquisition and transfer
- Corporations set up outside the PRC to acquire technology for a PRC intelligence service, corporation, or institute covertly
- Corporations set up outside the PRC by a PRC intelligence service, corporation, or institute solely to give cover to professional or non-professional agents who enter the United States to gather technology or for other purposes
- Corporations set up outside the PRC by a PRC intelligence service to launder money
- Corporations set up outside the PRC by a PRC intelligence service to raise capital to fund intelligence operations

- Corporations set up outside the PRC by a PRC individual to hide, accumulate, or raise money for personal use.
- Corporations set up outside the PRC by organs of the PRC Government to funnel money to key US leaders for the purpose of garnering favor and influencing the US political process and US Government decision-making

The differing meanings attached to the term "front companies" by different US agencies has led to confusion, particularly because many PRC companies fall into several different categories, at the outset or at different times during their existence. In addition, US agencies responsible for different aspects of national security, law enforcement, and Sino-US relations often do not share even basic data concerning PRC espionage in the United States.

This may partly explain why, for example, in Senate testimony on the same day in 1997, the State Department said it could identify only two PLA companies that were doing business in the United States, while the AFL-CIO identified at least 12, and a Washington-based think-tank identified 20 to 30 such companies.<sup>46</sup> The Select Committee has determined that all three figures are far below the true figure.

The Select Committee has concluded that there are more than 3,000 PRC corporations in the United States, some with links to the PLA, a State intelligence service, or with technology targeting and acquisition roles. The PRC's blurring of "commercial" and "intelligence" operations presents challenges to US efforts to monitor technology transfers for national security purposes.

General Liu Huaqing, who recently retired as a member of the Communist Party Politburo, the CCP Standing Committee, and the Central Military Commission, was involved with dozens of companies in Hong Kong and in Western countries engaged in illegally acquiring advanced US technology.



---

Yet another complicating factor is the evolution of the names used by PRC-controlled corporations. Some corporations such as NORINCO and Polytechnologies were easily recognizable as subsidiaries of PRC corporations. The boards of directors of PRC companies were also easily recognizable as PLA officers in the past.<sup>47</sup> Recent changes, however, have made it more difficult to recognize PRC corporations.

Some analysts note that US-based subsidiaries of PLA-owned companies in particular have stopped naming themselves after their parent corporation, a move prompted at least in part by criminal indictments and negative media reports that have been generated in connection with their activities in the United States. Many PLA-owned companies in the United States have simply ceased to exist in the past year or so, a phenomenon that reflects these factors as well as the fact that PRC-controlled companies often do not make money.<sup>48</sup>

The PRC intelligence services use front companies for espionage. These front companies may include branches of the large ministerial corporations in the PRC, as well as small one- and two-person establishments. Front companies, whatever the size, may have positions for PRC intelligence service officers. PRC front companies are often in money-making businesses that can provide cover for intelligence personnel in the United States.

PRC front companies may be used to sponsor visits to the US by delegations that include PRC intelligence operatives.

There has been increasing PRC espionage through front companies during the 1990s. As of the late 1990s, a significant number of front companies with ties to PRC intelligence services were in operation in the United States.

The PRC also uses its state-controlled “news” media organizations to gain political influence and gather political intelligence.

In June 1993, after a highly publicized trial, a former Chinese philosophy professor, Bin Wu,

and two other PRC nationals were convicted in a US court of smuggling third-generation night-vision equipment to the PRC. Wu worked at the direction of the MSS, which he says directed him to acquire numerous high-technology items from US companies. To accomplish these tasks, Wu and the others created several small front companies in Norfolk, Virginia. From that base, they solicited technology from a number of US companies, purchasing the equipment in the names of the front companies and forwarding it to the MSS through intermediaries in Hong Kong.<sup>49</sup>

Wu was a good example of the non-traditional PRC approach to acquiring technology in that Wu himself was not a professional intelligence agent. Identified as a pro-Western dissident by the MSS just after the Tiananmen Square massacre, he was given a choice: he could stay in the PRC and face prison, or he could accept the MSS’s offer to help him and his family by supporting the PRC in its quest for high technology. Wu was also a “sleeper” agent, who was initially told to go to the United States and establish himself in the political and business community. The MSS told Wu he would be called upon and given taskings later.<sup>50</sup>

Wu appears to have been part of a significant PRC intelligence structure in the United States. This structure includes “sleeper” agents, who can be used at any time but may not be tasked for a decade or more.<sup>51</sup>

In the 1990s, the PRC has also attempted to use front companies to acquire sensitive information on restricted military technologies, including the Aegis combat system. The Aegis combat system uses the AN/SPY-1 phased array radar to detect and track over 100 targets simultaneously, and a computer-based command and decision system allowing for simultaneous operations against air, surface, and submarine threats.<sup>52</sup>

### **Direct Collection of Technology by Non-Intelligence Agencies and Individuals**

PRC intelligence agencies often operate in the

---

US commercial environment through entities set up by other PRC Government and commercial organizations instead of creating their own fronts. PLA military intelligence officers do operate, however, directly in the United States, posing as military attaches at the PRC Embassy in Washington, D.C., and at the United Nations in New York.

Individuals attached to PRC Government and commercial organizations accomplish most PRC covert collection of restricted technology in the United States and are unaffiliated with official PRC intelligence services. These organizations collect their own technology from the United States, rather than rely on the PRC intelligence agencies to do it for them.

The Cox Committee judged that the MSS might be allowing other PRC Government entities to use MSS assets to fulfill their intelligence needs. These findings further illustrate that PRC “intelligence” operations are not necessarily conducted by what are traditionally thought of as “intelligence” agencies.

The main PLA intelligence activity in the United States is not represented by PLA intelligence organizations, but by PRC military industries and regular components of the PLA. Although military-industrial corporations are not PLA-owned, they are deeply involved in arms production and acquisition of military technology.

The activities of CATIC and its US subsidiaries exemplify the activities carried out by PRC military-industrial companies. Other PRC companies, such as China Great Wall Industry Corporation, collect technology for their own use and may be used as cover by PRC intelligence personnel.

Various science and technology commissions and organizations also carry out PRC technology acquisition in the United States. COSTIND, for example, has no official US subsidiary but is the primary coordinating authority over the military-industrial corporations that collect technology in

the United States. COSTIND also uses the “front company” device to procure high-technology products.

The PRC State Science and Technology Commission largely oversee civilian science and technology collection. The State Science and Technology Commission also use diplomats in the US as a key collection tool. It has provided funding to a PRC scientist to establish various commercial enterprises in the US as a means of collecting technology information for distribution in the PRC.

The State Science and Technology Commission was involved in efforts to elicit nuclear weapons information from a Chinese-American scientist. Science and Technology offices in the PRC’s seven diplomatic agencies in the United States carry out a substantial portion of technology acquisition taskings. The primary role of these offices is to arrange contacts between PRC scientists and their American counterparts.

Various “liaison groups” constitute another PRC technology collection vehicle in the United States. The PRC’s primary official liaison organization is the China Association for International Exchange of Personnel (CAIEP). CAIEP operates seven “liaison organization” offices in the United States, including one in Washington, D.C., and one in San Francisco. It is one of several organizations set up by the PRC to illegally acquire technology through contacts with Western scientists and engineers. Others include a purported technology company and a PRC State agency.

Another significant source of the PRC’s technology collection efforts outside of its formal intelligence agencies comes from Chinese business representatives loyal to the CCP who emigrate to the United States. These individuals pursue commercial interests independent of direct PRC Government control. Their primary motive is personal financial gain, and they will sell their efforts and opportunities to any willing consumer. When asked to do so, they pass US technology back to the PRC.

---

The PRC also acquires advanced technology through the outright theft of information. A few cases exemplify this method of technology acquisition of which the Peter Lee case represents a classic non-intelligence service operation.

Peter Lee is a naturalized US citizen who was born in Taiwan. Lee worked at Los Alamos National Laboratory from 1984 to 1991, and for TRW Inc., a contractor to Lawrence Livermore National Laboratory, from 1973 to 1984 and again from 1991 to 1997.

Lee has admitted to the FBI that, in 1997, he passed to PRC weapons scientists classified research into the detection of enemy submarines under water. This research, if successfully completed, could enable the PLA to threaten previously invulnerable US nuclear submarines.

Lee made the admissions in 1997 during six adversarial interviews with the FBI. According to Lee, the illegal transfer of this sensitive research occurred while he was employed by TRW, Inc., a contractor for the Lawrence Livermore National Laboratory. Lawrence Livermore developed the classified information as part of a joint US-United Kingdom Radar Ocean Imaging project for anti-submarine warfare applications.

In 1997, the decision was made to not prosecute Lee for passing this classified information on submarine detection to the PRC. Because of the sensitivity of this area of research, the Defense Department requested that this information not be used in a prosecution.

Throughout much of the 1990s, the FBI conducted a multi-year investigation of Peter Lee, employing a variety of techniques, but without success in collecting incriminating evidence. Finally, in 1997, Lee was charged with willfully providing to the PRC classified information on techniques for creating miniature nuclear fusion explosions.

Specifically, Lee explained to PRC weapons scientists how deuterium and tritium can be loaded into a spherical capsule called a target and

surrounded by a “hohlraum,” and then heated by means of laser bombardment. The heat causes the compression of these elements, creating a nuclear fusion micro-explosion. This so-called “inertial confinement” technique permits nuclear weapons scientists to study nuclear explosions in miniature—something of especial usefulness to the PRC, which has agreed to the ban on full-scale nuclear tests in the Comprehensive Test Ban Treaty.

Lee said that during a lecture in the PRC he answered questions and drew diagrams about hohlraum construction. In addition, Lee is believed to have provided the PRC with information about inertial confinement lasers that are used to replicate the coupling between the primary and secondary in a thermonuclear weapon.

Lee was formally charged with one count of “gathering, transmitting or losing defense information,” in violation of Section 793 of Title 18 of the US Code, and one count of providing false statements to a US government agency, in violation of Section 1001, Title 18. On December 8, 1997, Lee pled guilty to willfully passing classified US defense information to PRC scientists during his 1985 visit to the PRC. Lee also pled guilty to falsifying reports of contact with PRC nationals in 1997. Lee was sentenced to 12 months in a halfway house, a \$20,000 fine and 3,000 hours of community service.<sup>53</sup>

The Cox Committee judged that, between 1985 and 1997, Lee might have provided the PRC with more classified thermonuclear weapons-related information than he has admitted. The PRC apparently co-opted Lee by appealing to his ego, his ethnicity, and his sense of self-importance as a scientist.

The Cox Committee also received evidence of PRC theft of technology data from US industry during the 1990s valued at millions of dollars. The PRC used Chinese nationals hired by US firms for that purpose. The Clinton administration has determined that no details of this evidence may be made public without affecting national security.

---

In 1993, PRC national Yen Men Kao, a North Carolina restaurant owner, was arrested by the FBI and charged with conspiring to steal and export classified and export-controlled high-technology items to the PRC.<sup>54</sup> Among the items about which Kao and several other PRC nationals were seeking information were:

- The US Navy's Mark 48 Advanced Capability Torpedo
- The F-404 jet engine used on the US F-18 Hornet fighter
- The fire-control radar for the US F-16 fighter<sup>55</sup>

The case of Kao and his co-conspirators is one of several involving PRC commercial entities attempting to illegally acquire US technology.

The PRC also relies heavily on the use of professional scientific visits, delegations, and exchanges to gather sensitive technology.

As the PRC Government has increasingly participated in the world commercial and capital markets, the number of PRC representatives entering the United States has increased dramatically. One estimate is that in 1996 alone, more than 80,000 PRC nationals visited the United States as part of 23,000 delegations.

Almost every PRC citizen allowed to go to the United States as part of these delegations likely receives some type of collection requirement, according to official sources.

Scientific delegations from the PRC are a typical method used by the PRC to begin the process of finding US joint venture partners. These delegations have been known to go through the motions of establishing a joint venture to garner as much information as possible from the US partner, only to pull out at the last minute.

Scientific visits and exchanges by PRC scientists and engineers and their US counterparts create several risks to US national security. This has been a particular concern in recent years regarding

foreign visitors to the Department of Energy's national weapons laboratories.<sup>56</sup>

The first of these risks is that visitors to US scientific and technology sites may exploit their initial, authorized access to information to gain access to protected information.<sup>57</sup> The Cox Committee reviewed evidence of PRC scientists who circumvented US restrictions on their access to sensitive manufacturing facilities.

Another risk is that US scientists may inadvertently reveal sensitive information during professional discussions.

The PRC subjects visiting scientists to a variety of techniques designed to elicit information from them. One technique may involve inviting scientists to make a presentation in an academic setting, where repeated and increasingly sensitive questions are asked.<sup>58</sup> Another is to provide the visitor with sightseeing opportunities while PRC intelligence agents burglarize the visitor's hotel room for information. Still another technique involves subjecting the visitor to a grueling itinerary and providing copious alcoholic beverages so as to wear the visitor down and lower resistance to questions.<sup>59</sup>

In one instance, a US scientist traveled to the PRC where very specific technical questions were asked. The scientist, hesitant to answer one question directly because it called for the revelation of sensitive information, instead provided a metaphorical example. The scientist immediately realized that the PRC scientists grasped what was behind the example, and knew that too much had been said.

Another common PRC tactic is to tell US visitors about the PRC's plan for further research, the hope being that the US scientist will release information in commenting on the PRC's plans.

The Cox Committee reviewed evidence of this technique being applied to acquire information to assist the PRC in creating its next generation of nuclear weapons.

---

Another risk inherent in scientific exchanges is that US scientists who are overseas in the PRC are prime targets for approaches by professional and non-professional PRC organizations that would like to co-opt them into assisting the PRC. In many cases, they are able to identify scientists whose views might support the PRC, and whose knowledge would be of value to PRC programs.

The Cox Committee received information about Chinese-American scientists from US nuclear weapons design laboratories being identified in this manner. Typically, the PRC will invite such a scientist to lecture and, once in the PRC, question him closely about his work. Once the scientist has returned to the US, answers to follow-up questions may be delivered through a visiting intermediary. Such efforts to co-opt scientists may be conducted by PRC ministries, and may involve COSTIND.

The number of PRC nationals attending educational institutions in the United States presents another opportunity for the PRC to collect sensitive technology.<sup>60</sup> It is estimated that at any given time there are over 100,000 PRC nationals who either are attending US universities or have remained in the United States after graduating from a US university. These PRC nationals provide a ready target for PRC intelligence officers and PRC Government-controlled organizations, both while they are in the United States and when they return to the PRC.<sup>61</sup>

The Cox Committee judged that the PRC was increasingly looking to PRC scholars who remain in the United States as assets who have developed a network of personal contacts that can be helpful to the PRC's search for science and technology information.

The PRC has also acquired technological information through open forums such as arms exhibits and computer shows. During one international arms exhibit, for example, PRC nationals were observed collecting all possible forms of technical information. This included videotaping every static display and designating individuals to take notes. The group also stole a

videocassette from a display that was continuously playing information on the US Theater High Altitude Air Defense system, when the Defense Department contractor left it unattended. Converting the stolen cassette to a frame-by-frame sequence could yield valuable intelligence information to the PRC.<sup>62</sup>

### **Illegal Export of Military Technology Purchased in the United States**

The PRC is also taking advantage of the ongoing US military downsizing. In particular, PRC representatives and companies in the United States pursue the purchase of high-technology US military surplus goods.

In a single 1996-1997 operation, the Los Angeles office of the US Customs Service seized over \$36 million in excess military property that was being shipped overseas illegally. Among the seized US military surplus equipment on its way to the PRC and Hong Kong were:

- 37 inertial navigation systems for the US F-117 and FB-111 aircraft
- Thousands of computers and computer disks containing classified Top Secret and higher information
- Patriot missile parts
- 500 electron tubes used in the US F-14 fighter
- Tank and howitzer parts
- 26,000 encryption devices.<sup>63</sup>

PRC representatives have been the biggest buyers of sensitive electronic surplus material. Defense Department investigators have noted a trend among the PRC buyers of this equipment: many had worked for high-technology companies in the PRC or for PRC Government science and technology organizations.<sup>64</sup>

The PRC has been able to purchase these goods because, in its rush to dispose of excess property, the Defense Department failed to code properly or to disable large amounts of advanced military equipment, allowing PRC buyers to pay for and take immediate possession of functional high-



---

technology equipment. Often this equipment was purchased as “scrap,” for which the buyers paid pennies on the dollar.<sup>65</sup>

According to the US Customs Service, many PRC companies that bid on military surplus technology intentionally used “American-sounding” names to mask their PRC affiliation.<sup>66</sup>

The PRC also has been able to exploit US military downsizing by purchasing advanced technology, in the form of machine tools and production equipment from decommissioned US defense factories, through industrial auctions.

For example, a multi-axis machine tool profiler, designed to build wing spans for the US F-14 fighter, originally cost over \$3 million but was purchased by the PRC for under \$25,000.<sup>67</sup>

According to one industrial auctioneer, the PRC frequents industrial auctions because they offer accurate, well-maintained equipment at bargain prices and with quick delivery.<sup>68</sup> Moreover, once the PRC obtains this equipment, there are ample resources available in the United States to upgrade the equipment to modern standards.

A California company specializing in refurbishing machine tools, for example, was approached in recent years by representatives of CATIC’s El Monte, California office. The CATIC representatives reportedly inquired about the scope of the company’s refurbishment capability, including whether it could train CATIC people to rebuild and maintain the machines and whether the company would be willing to assemble the machines in the PRC. The CATIC personnel also reportedly asked if the company could convert a three-axis machine tool to a five-axis machine tool. They were told this was possible for some machines, and very often only requires replacing one computer controller with another.<sup>69</sup>

The US company noted, however, that such a converted machine would require an export license. In response, the CATIC personnel reportedly said, rather emphatically, that they would have

“no problem” with the export. The CATIC inquiries came at about the same time CATIC was negotiating the purchase of machine tools from the McDonnell Douglas Columbus, Ohio plant.

CATIC’s discussions with this particular US company did not result in either the training of CATIC personnel or the conversion of any machine tools. It is unknown, however, what other US companies were approached with similar inquiries or whether any such inquiries resulted in technological assistance to CATIC or the PRC.

The Cox Committee reviewed evidence from the mid-1990s of a PRC company that obtained US defense manufacturing technology for jet aircraft, knowingly failed to obtain a required export license, and misrepresented the contents of its shipping containers in order to get the technology out of the country. The Clinton administration determined that further information on this case could not be made public without affecting national security.

## **PRC Purchase of Interests in US Companies**

A more recent method used by the PRC to obtain advanced technology from the United States is through the purchase of an interest in US high-technology companies or US export facilities. While this method does not yet appear to be prevalent, it has been identified in at least three instances.

In 1990, CATIC acquired an interest in MAMCO Manufacturing, a Seattle, Washington aircraft parts manufacturer. In a highly-publicized decision that year, President George Bush exercised his authority under section 721 of the Defense Production Act of 1950 (also known as the Exon-Florio provision) to order CATIC to divest itself of its MAMCO interest. This was based on the recommendations of the Committee on Foreign Investment in the United States (CFIUS), an inter-agency committee chaired by the Secretary of Treasury and tasked to conduct

---

reviews of foreign acquisitions that might threaten national security.<sup>70</sup>

CFIUS concluded that:

- Some technology used by MAMCO, although not state-of-the-art, was export-controlled
- CATIC had close ties to the PLA through the PRC Ministry of Aviation (now known as AVIC)
- The acquisition would give CATIC unique access to US aerospace companies

It is likely that the PRC's strategy in acquiring MAMCO was to give CATIC a venue from which to solicit business with US aerospace firms, both to yield revenue and to gain access to aerospace technologies, inasmuch as CATIC has conspired to illegally acquire US sensitive technology in the past. In addition, according to public reports, CATIC has been used for PRC arms sales to countries such as Iran.

The PRC's efforts to acquire MAMCO did not end with President Bush's divestiture order. CATIC requested CFIUS approval to satisfy the concerns expressed in President Bush's divestiture order by selling its MAMCO interest to CITIC.

CFIUS noted that CITIC reported directly to the highest level of the PRC Government, the PRC State Council, and that CITIC did not have any colorable business rationale for wanting to acquire MAMCO. When CFIUS began questioning CITIC's business purposes and its ties to the State Council, CATIC withdrew its request.

CATIC then filed another request, this time proposing that it meet President Bush's divestiture order by selling its MAMCO interest to Huan-Yu Enterprises, a PRC company that was owned by a PRC provincial government and reported to the PRC MEI (now known as the Ministry of Information Industry), which in turn reported directly to the PRC State Council.

A CFIUS investigation concluded that Huan-Yu was a consumer, not a producer, of aerospace parts

and had no legitimate reason to acquire MAMCO. The proposed divestiture looked to CFIUS like a "sham acquisition." Faced with intense CFIUS interest, CATIC again withdrew its filing.

In 1996, Sunbase Asia, Incorporated purchased Southwest Products Corporation, a California producer of ball bearings for US military aircraft. Sunbase is incorporated in the United States, but is owned by an investment group comprised of some of the PRC's largest state-owned conglomerates as well as a Hong Kong company. According to a Southwest executive, the purchase will "take [Sunbase] to the next level" of technology.<sup>71</sup> The Clinton administration determined that additional information on this transaction could not be made public without affecting national security.

China Ocean Shipping Company (COSCO), the PRC's state-owned shipping company which operates under the direction of the Ministry of Foreign Trade and Economic Cooperation and answers to the PRC State Council,<sup>72</sup> attempted to lease port space that was being vacated by the US Navy in Long Beach, California. The lease proposal led to a heated debate between Congress, which wanted to prevent the lease based on national security concerns, and President Clinton, who supported the lease. Legislation passed by both houses of Congress in 1997 barred the lease and voided the President's authority to grant a waiver.<sup>73</sup>

Other information indicates COSCO is far from benign. In 1996, US Customs agents confiscated over 2,000 assault rifles that were being smuggled into the United States aboard COSCO ships.<sup>74</sup> "Although presented as a commercial entity," according to the House Task Force on Terrorism and Unconventional Warfare, "COSCO is actually an arm of the Chinese military establishment." The Clinton administration determined that additional information concerning COSCO that appeared in the Cox Committee's classified Final Report could not be made public without affecting national security.

---

## Methods Used by the PRC to Export Military Technology from the United States

Once the PRC acquires advanced technology in the United States, it requires secure means to export the information or hardware out of the country. Weaknesses in US customs can be exploited to smuggle classified or restricted US technology.

Diplomatic pouches and traveling PRC diplomats offer another avenue for illegal technology exports. Almost every PRC Government commercial and diplomatic institution in the United States has personnel who facilitate science and technology acquisitions.

The Cox Committee believed that these means of communicating with the PRC could have been exploited to smuggle nuclear weapons secrets from the United States.

These are some of the further means that have been used to illegally ship sensitive technology to the PRC:

- In 1993, Bin Wu, a PRC national, was convicted of transferring night-vision technology to the PRC. Wu used the US postal system to get technology back to the PRC. He mailed the technology he collected directly to the PRC, mostly through an intermediary in Hong Kong.<sup>75</sup>
- The PRC uses false exportation documentation and has falsified end-user certificates. In one case reviewed by the Select Committee, the Department of Commerce reported that a US subsidiary of a PRC company used a common illegal export tactic when it falsely identified the machine tools it was exporting. The US Customs Service also indicated that the PRC's use of false bills of sale and false end-use statements are common illegal export tactics.
- The PRC has used at least one commercial air carrier to assist in its technology transfer efforts. In 1996, Hong Kong Customs officials intercepted air-to-air missile parts being shipped

by CATIC aboard a commercial air carrier, Dragonair. Dragonair is owned by CITIC, the most powerful and visible PRC-controlled conglomerate, and Civil Aviation Administration of China (CAAC).<sup>76</sup>

- A common PRC method for transferring US technology to the PRC uses Hong Kong as the shipment point. This method takes advantage of the fact that US export controls on Hong Kong are significantly less restrictive than those applied to the rest of the PRC, allowing Hong Kong far easier access to militarily-sensitive technology.

The more relaxed controls on the export of militarily sensitive technology to Hong Kong have been allowed to remain in place even though Hong Kong was absorbed by the PRC and PLA garrisons took control of the region on July 1, 1997. US trade officials report that no inspections by the Hong Kong regional government or by any other government, including the United States, are permitted when PLA vehicles cross the Hong Kong border.

Various US Government analyses have raised concerns about the risk of the diversion of sensitive US technologies not only to the PRC, but to third countries as well through Hong Kong because of the PRC's known use of Hong Kong to obtain sensitive technology.<sup>77</sup> Some controlled dual-use technologies can be exported from the United States to Hong Kong license-free, even though they have military applications that the PRC would find attractive for its military modernization efforts.

The Cox Committee reported indications that a sizeable number of Hong Kong enterprises serve as cover for PRC intelligence services, including the MSS. Therefore, it is likely that over time, these could provide the PRC with a much greater capability to target US interests in Hong Kong.

US Customs officials also concur that transshipment through Hong Kong is a common PRC tactic for the illegal transfer of technology.<sup>78</sup>

---

## **PRC Incentives for US Companies to Advocate Relaxation of Export Controls**

US companies in the high-technology sector are eager to access the PRC market. The PRC often requires these US firms to transfer technologies to the PRC as a precondition to market access. US export regulations can be seen as an impediment to commercial opportunities.<sup>79</sup>

Executives wishing to do business in the PRC share a mutual commercial interest with the PRC in minimizing export controls on dual-use and military-related commodities. The PRC has displayed a willingness to exploit this mutuality of interest in several notoriously public cases by inducing VIPs from large US companies to lobby on behalf of initiatives, such as export liberalization, on which they are aligned with the PRC.

The PRC is determined to reduce restrictions on the export of US communications satellites for launch in the PRC. From the perspective of the PRC, provision of such launch services creates a unique opportunity to consult with US satellite manufacturers, access information regarding US satellite technology, and obtain resources to modernize their rockets.<sup>80</sup> US satellite manufacturers are, in turn, anxious to access the potentially lucrative PRC market, and realize that launching in the PRC is a potential condition to market access.<sup>81</sup>

By agreeing to procure numerous satellites from Hughes Electronics Co. (Hughes) and Space Systems/Loral (Loral) in the early 1990s, the PRC created a mutuality of interest with two companies well-positioned to advocate the liberalization of export controls on these platforms.

For example, Bernard L. Schwartz, Chairman and CEO of Loral Space & Communications, Ltd., the parent company of Loral, met directly on at least four occasions with Secretary of Commerce Ron Brown after 1993, and accompanied him on a 1994 trade mission to the PRC.<sup>82</sup>

C. Michael Armstrong, the former Chairman and Chief Executive Officer of GM Hughes Electronics, the parent company of Hughes, has served as Chairman of President Clinton's Export Council since 1993, working with the Secretary of State, the Secretary of Commerce, and others to "provide insight and counsel" to the President on a variety of trade matters.<sup>83</sup> Armstrong also served or had served as a member of the Defense Preparedness Advisory Council, the Telecommunications Advisory Council, and the Secretary of State's Advisory Council.<sup>84</sup>

Both Armstrong and Schwartz, as well as other executives from high-technology firms, advocated the transfer of export licensing authority from the "more stringent control" of the State Department to the Commerce Department. Armstrong met with the Secretary of Defense, the National Security Advisor, and the Secretary of State on the matter, and both Schwartz and Armstrong co-signed a letter with Daniel Tellep of Lockheed-Martin Corporation to the President urging this change.<sup>85</sup> The changes they advocated were ultimately adopted.

Between 1993 and January 3, 1999, Loral and Hughes succeeded in obtaining waivers or export licenses for an aggregate of five satellite projects.<sup>86</sup>

Another example of the incentive to advocate the relaxation of export controls involved the Charoen Pokphand Group (CP Group), Thailand's largest multinational company and one of the largest investors in the PRC. CP Group executives have served as economic advisors to the PRC Government and were chosen to sit on the committees dealing with the absorption of Hong Kong.<sup>87</sup>

The CP Group was a founding member of Asia Pacific Telecommunications Satellite Holdings, Ltd. (APT), a consortium run by PRC-controlled investment companies, including China Aerospace Corporation. APT imports satellites manufactured by Hughes and Loral as part of the Apstar program for launch in the PRC by China Great Wall Industry Corporation.<sup>88</sup>

---

On June 18, 1996, several CP Group executives attended a coffee with President Clinton at the White House. These executives included Dhanin Chearavanont (CP Chairman and Chief Executive Officer), Sumet Chearavanont (Vice Chairman and President), and Sarasin Virapol (employee and translator). The CP executives were invited to the coffee by their Washington, D.C., lobbyist, Pauline Kanchanalak.<sup>89</sup>

According to one participant, Karl Jackson of the US-Thailand Business Council, the CP executives “dominated the conversation at the coffee.” The discussion included US-PRC relations, Most-Favored-Nation trade status for the PRC, and US technology. Other participants corroborate Jackson’s characterization of the role that CP executives played at the event.<sup>90</sup>

### **PRC Theft of US Thermonuclear Warhead Design Information**

The People’s Republic of China’s penetration of our national weapons laboratories spans at least the past several decades, and almost certainly continues today.

The PRC’s nuclear weapons intelligence collection efforts began after the end of the Cultural Revolution in 1976, when the PRC assessed its weaknesses in physics and the deteriorating status of its nuclear weapons programs.

The PRC’s warhead designs of the late 1970s were large, multi-megaton thermonuclear weapons that could only be carried on large ballistic missiles and aircraft. The PRC’s warheads were roughly equivalent to US warheads designed in the 1950s. The PRC may have decided as early as that time to pursue more advanced thermonuclear warheads for its new generation of ballistic missiles.

The PRC’s twenty-year intelligence collection effort against the US has been aimed at this goal. The PRC employs a “mosaic” approach that capitalizes on the collection of small bits of

information by a large number of individuals, which is then pieced together in the PRC. This information is obtained through espionage, rigorous review of US unclassified technical and academic publications, and extensive interaction with Department of Energy (DOE) laboratories and US scientists.

The Cox Committee judged that the PRC’s intelligence collection efforts to develop modern thermonuclear warheads were focused primarily on the Los Alamos, Lawrence Livermore, Sandia, and Oak Ridge National Laboratories.

As a result of these efforts, the PRC has stolen classified US thermonuclear design information that helped it fabricate and successfully test a new generation of strategic warheads.

The PRC stole classified information on every currently deployed US intercontinental ballistic missile (ICBM) and submarine-launched ballistic missile (SLBM). The warheads for which the PRC stole classified information include: the W-56 Minuteman II ICBM; the W-62 Minuteman III ICBM; the W-70 Lance short-range ballistic missile (SRBM); the W-76 Trident C-4 SLBM; the W-78 Minuteman III Mark 12A ICBM; the W-87 Peacekeeper ICBM; and the W-88 Trident D-5 SLBM. The W-88 warhead is the most sophisticated strategic nuclear warhead in the US arsenal. It is deployed on the Trident D-5 submarine-launched missile.

The PRC also stole classified information on US weapons design concepts, on weaponization features, and on warhead reentry vehicles (the hardened shell that protects a warhead during reentry).



---

The PRC may have acquired detailed documents and blueprints from the US national weapons laboratories.

The US Intelligence Community reported in 1996 that the PRC stole neutron bomb technology from a US national weapons laboratory. The PRC had previously stolen design information on the US W-70 warhead in the late 1970s; that earlier theft, which included design information, was discovered several months after it took place. The W-70 has elements that can be used as a strategic thermonuclear warhead or an enhanced radiation (“neutron bomb”) warhead. The PRC tested a neutron bomb in 1988.

The PRC may have also acquired classified US nuclear weapons computer codes from US national weapons laboratories. The Cox Committee believed that nuclear weapons computer codes remain a key target for PRC espionage. Nuclear weapons codes are important for understanding the workings of nuclear weapons and can assist in weapon design, maintenance, and adaptation. The PRC could make use of this information, for example, to adapt stolen US thermonuclear design information to meet the PRC’s particular needs and capabilities.

During the mid-1990s, it was learned that the PRC had acquired US technical information about insensitive high explosives. Insensitive high explosives are a component of certain thermonuclear weapons. Insensitive high explosives are less energetic than high explosives used in some other thermonuclear warheads, but have advantages for other purposes, such as thermonuclear warheads used on mobile missiles.

The PRC thefts from our national weapons laboratories began at least as early as the late 1970s, and significant secrets are known to have been stolen as recently as the mid-1990s. Such thefts almost certainly continue to the present.

### **How the PRC Acquired Thermonuclear Warhead Design Information from the United States: PRC Espionage and Other PRC Techniques**

The Cox Committee judged that the PRC’s intelligence collection efforts to develop modern thermonuclear warheads focused primarily on the following US National Laboratories: Los Alamos, Lawrence Livermore, Oak Ridge, and Sandia. These efforts included espionage, rigorous review of US unclassified technical and academic publications, and extensive interaction with Department of Energy laboratories and US scientists.

Espionage played a central part in the PRC’s acquisition of classified US thermonuclear warhead design secrets. In several cases, the PRC identified lab employees, invited them to the PRC, and approached them for help, sometimes playing upon ethnic ties to recruit individuals.

The PRC also rigorously mined unclassified technical information and academic publications, including information from the National Technical Information Center and other sources. PRC scientists have even requested reports via e-mail from scientists at the US national weapons laboratories. Peter Lee, who had been a scientist at both Lawrence Livermore and Los Alamos National Laboratories and was convicted in 1997 of passing classified information to the PRC, gave the PRC unclassified technical reports upon request. The PRC also learned about conventional explosives for nuclear weapon detonation from reviewing unclassified technical reports published by Department of Energy national weapons laboratories.

PRC scientists have used their extensive laboratory-to-laboratory interactions with the United States to gain information from US scientists on common problems, solutions to nuclear weapons physics, and solutions to engineering problems. The PRC uses elicitation in these meetings, where it shows familiarity with US information in an effort to “prime the pump” in order to try to glean

---

information about US designs. US scientists have passed information to the PRC in this way that is of benefit to the PRC's nuclear weapons program.

The PRC's espionage operations, which use traditional intelligence gathering organizations as well as other entities, are aggressively focused on US weapons technology.

The PRC's Academy of Engineering Physics (CAEP), which is under COSTIND, is the entity in charge of the PRC's nuclear weapons program. It is responsible for the research and development, testing, and production of all of the PRC's nuclear weapons.

CAEP has pursued a very close relationship with US national weapons laboratories, sending scientists as well as senior management to Los Alamos and Lawrence Livermore. Members of CAEP's senior management have made at least two trips during the mid-to-late 1990s to US national weapons laboratories to acquire information and collect intelligence. These visits provided the opportunity for the PRC to collect intelligence. The presence of such PRC nationals at the US national weapons laboratories facilitated the PRC's targeting of US weapons scientists for the purpose of obtaining nuclear weapons information.

US and PRC lab-to-lab exchanges were ended in the late 1980s, but were resumed in 1993. Scientific exchanges continue in many areas including high-energy physics.<sup>91</sup> Discussions at the US national weapons laboratories in connection with the foreign visitors program are supposed to be strictly limited to technical arms control and material accounting issues. Nonetheless, these visits and scientific conferences provide opportunities for the PRC to interact with US scientists outside of official meetings, and facilitate the PRC's targeting of US weapons scientists.

The US national weapons laboratories argue that there are reciprocal gains from the exchanges. DOE describes some of the insights gained from these exchanges as unique. On the other hand, PRC scientists have misled the US about their

objectives and technological developments. Despite considerable debate in Congress and the Executive branch, including several critical GAO reports, the US Government has never made a definitive assessment of the risks versus the benefits of scientific exchanges and foreign visitor programs involving the US national weapons laboratories.<sup>92</sup>

### **How the US Government Learned of the PRC's Theft of Our Most Advanced Thermonuclear Warhead Design Information**

The US Government did not become fully aware of the magnitude of the counterintelligence problems at DOE laboratories until 1995. The first indication of successful PRC espionage against the laboratories arose in the late 1970s. During the last several years, more information has become available concerning thefts of US thermonuclear warhead design information, and how the PRC may be exploiting it. A series of PRC nuclear tests conducted from 1992 to 1996 that furthered the PRC's development of advanced warheads led to suspicions in the US intelligence community that the PRC had stolen advanced US thermonuclear warhead design information.

### **The "Walk-In"**

In 1995, a "walk-in" approached the CIA outside of the PRC and provided an official PRC document classified "Secret" that contained design information on the W-88 Trident D-5 warhead, the most modern in the US arsenal, as well as technical information concerning other thermonuclear warheads.

The CIA later determined that the "walk-in"<sup>93</sup> was directed by the PRC intelligence services. Nonetheless, the CIA and other Intelligence Community analysts that reviewed the document concluded that it contained US thermonuclear warhead design information. The "walk-in" document recognized that the US nuclear warheads

---

represented the state-of-the-art against which PRC thermonuclear warheads should be measured.

Over the following months, a multidisciplinary group from the US Government, including the DOE and scientists from the US national weapons laboratories, assessed the information in the document. DOE and FBI investigations focused on the loss of the US W-88 Trident D-5 design information, but they did not focus on the loss of technical information about the other five US thermonuclear warheads. A DOE investigation of the loss of technical information about the other five US thermonuclear warheads had not begun as of January 3, 1999, after the Cox Committee had completed its investigation. In addition, the FBI had not yet initiated an investigation as of January 3, 1999.

DOE reported that the PRC has in fact acquired some US computer codes, including: the MCNPT code; the DOT3.5 code; and the NJOYC code.<sup>9</sup> MCNPT is a theoretical code that is useful in determining survivability of systems to electronic penetration and dose penetration in humans. DOT3.5 is a two-dimensional empirical code that performs the same kinds of calculations as MCNPT, except uses numerical integration. NJOYC acts as a numerical translator between DOT3.5 and MCNPT.

Given the limited number of nuclear tests that the PRC has conducted, the PRC likely needs additional empirical information about advanced thermonuclear weapon performance that it could obtain by stealing the US “legacy” computer codes, such as those that were used by the Los Alamos National Laboratory to design the W-88 Trident D-5 warhead. The PRC may also need information about dynamic three-dimensional data on warhead packaging, primary and secondary coupling, and the chemical interactions of materials inside the warhead over time.

The Cox Committee was concerned that no procedures were in place that would either prevent or detect the movement of classified information, including classified nuclear-weapons design

information or computer codes, to unclassified sections of the computer systems at US national weapons laboratories. The access granted to individuals from foreign countries, including students, to these unclassified areas of the US national weapons laboratories’ computer systems could make it possible for others acting as agents of foreign countries to access such information, making detection of the persons responsible for the theft even more difficult.

The Cox Committee believed that the PRC would continue to target its collection efforts not only on Los Alamos National Laboratory, but also on the other US National Laboratories involved with the US nuclear stockpile maintenance program. The PRC may also seek to improve its hydrostatic testing capabilities by learning more about the Dual-Axis Radiographic Hydrotest (DARHT) facility at Los Alamos.

### **US Government Investigations of Nuclear Weapons Design Information Losses**

The Cox Committee received information about the US Government’s investigation of the PRC’s theft of classified US design information for the W-70 thermonuclear warhead. The W-70, which is an enhanced radiation nuclear warhead (or “neutron bomb”, also, has elements that can be used for a strategic thermonuclear warhead. In 1996, the US Intelligence Community reported that the PRC had successfully stolen classified US technology from a US Nuclear Weapons Laboratory about the neutron bomb.

This was not the first time the PRC had stolen classified US information about the neutron bomb. In the late 1970s, the PRC stole design information on the US W-70 warhead from Lawrence Livermore Laboratory. The US Government first learned of this theft several months after it took place. The PRC subsequently tested a neutron bomb in 1988.

The FBI developed a suspect in the earlier theft. The suspect worked at Lawrence Livermore National Laboratory, and had access to classified information including designs for a number of US thermonuclear weapons in the US stockpile at that time.

---

In addition to design information about the W-70, this suspect may have provided to the PRC additional classified information about other US weapons that could have significantly accelerated the PRC's nuclear weapons program.

### **Investigation of Theft of Design Information For the W-88 Trident D-5 Thermonuclear Warhead**

The Cox Committee received information about the US Government's ongoing investigation of the loss of information about the W-88 Trident D-5 thermonuclear warhead design.

During the PRC's 1992 to 1996 series of advanced nuclear weapons tests, a debate began in the US Government about whether the PRC had acquired classified US thermonuclear weapons design information. DOE began to investigate. In 1995, following the CIA's receipt of evidence (provided by the PRC-directed "walk-in") that the PRC had acquired technical information on a number of US thermonuclear warheads, including not only the W-88 Trident D-5 but five other warheads as well, DOE's investigation intensified. That investigation, however, focused on the W-88 and not the other weapons.

Early in its investigation, DOE cross-referenced personnel who had worked on the design of the W-88 with those who had traveled to the PRC or interacted with PRC scientists. One individual who had hosted PRC visitors in the past emerged from this inquiry as a suspect by the spring of 1995. (Editor Note: *Although the Cox Committee did not refer to the suspect by name because of the ongoing investigation, Wen Ho Lee was later identified as the suspect.*)

Even after being identified as a suspect, the individual, who still had a security clearance, continued to work in one of the most sensitive divisions at Los Alamos National Laboratory, Division X, which handles thermonuclear weapons designs and computer codes. In this position, the suspect requested and received permission to hire a

PRC graduate student who was studying in the US for the summer.

In December 1998, the suspect traveled to Taiwan. Following his return from Taiwan in December 1998, he was removed from Division X.

The FBI initiated a full investigation in the middle of 1996. At the date of the Cox Committee's January 3, 1999 classified Final Report, the suspect continued to work at the Los Alamos National Laboratory, and continued to have access to classified information. (Editor Note: *See Wen Ho Lee and also Department of Energy, FBI, and Department of Justice Handling of the Espionage Investigation into the Compromise of Design Information on the W-88 Warhead elsewhere in the CI Reader.*)

### **Investigation of Additional Incidents**

The Cox Committee reviewed one case that offers a troublesome example of the manner in which scientific exchanges in the PRC can be exploited for espionage purposes. The incident involved the inadvertent, bordering on negligent, disclosure of classified technical information by a US scientist lecturing in the PRC.

The US scientist, who was representing a US National Laboratory during a lab-to-lab exchange with a PRC laboratory, was pressured by PRC counterparts to provide a solution to a nuclear weapons-related problem. Rather than decline, the scientist, who was aware of the clear distinction between the classified and unclassified technical information that was under discussion, provided an analogy. The scientist immediately saw that the PRC scientists had grasped the hint that was provided and realized that too much had been said.

The PRC employs various approaches to co-opt US scientists to obtain classified information. These approaches include: appealing to common ethnic heritage; arranging visits to ancestral homes and relatives; paying for trips and travel in the PRC; flattering the guest's knowledge and intelligence;

---

holding elaborate banquets to honor guests; and doggedly peppering US scientists with technical questions by experts, sometimes after a banquet at which substantial amounts of alcohol have been consumed.

On average, the FBI has received about five security-related referrals each month from DOE. Not all of these concern the PRC. These referrals usually include possible security violations and the inadvertent disclosure of classified information. The FBI normally conducts investigations of foreign individuals working at the National Laboratories.

### **The Department of Energy's Counterintelligence Program at the US National Weapons Laboratories**

With additional funds provided by Congress in 1998, DOE is attempting to reinvent its counterintelligence programs at the US national weapons laboratories to prevent continued loss of information to the PRC's intelligence collection activities.

Funding for DOE's counterintelligence program, including seven employees at DOE's headquarters, was \$7.6 million in Fiscal Year 1998. For Fiscal Year 1999, Congress has increased that amount to \$15.6 million. With the support of the Director of Central Intelligence and the Director of the FBI, the President issued Presidential Decision Directive 61 (PDD-61) in February 1998. PDD-61 requires that a senior FBI counterintelligence agent be placed in charge of DOE's program, which has been done.

PDD-61 also instructed that a counterintelligence report with recommendations be presented to the Secretary of Energy. The report was submitted to the Secretary on July 1, 1998, with 33 specific recommendations. The Secretary had 30 days to respond to the NSC. However, due to the transition from Secretary Pena to Secretary Richardson, the response was delayed. In late November 1998, the Secretary of Energy approved all substantive recommendations. In December 1998, the

Directors of the US National Laboratories agreed to the counterintelligence plan during a meeting with the Secretary of Energy. DOE is now implementing the plan.

The Secretary's action plan instructs the Directors of the US National Laboratories to implement the recommendations. It directs DOE's Office of Counterintelligence to fund counterintelligence positions at individual laboratories so that they work directly for DOE, not the contractors that administer the laboratories.

DOE was to create an audit trail to track unclassified computer use and protect classified computer networks. The action plan also directed the creation of counterintelligence training programs and a counterintelligence analysis program. (Editor's Note: *See The Redmond Report, which reviewed the counterintelligence program at the Labs.*)

The DOE was also implement stricter requirements for reporting all interactions with foreign individuals from sensitive countries, including correspondence by e-mail. Laboratory Directors would be responsible for scrutinizing foreign visitors, in coordination with DOE's Counterintelligence Office.

DOE would require counterintelligence polygraphs of those who work in special access programs (SAP) and sensitive areas with knowledge of nuclear weapons design, or actually have hands-on access to nuclear weapons (about 10 percent of the total cleared population within DOE. Such persons would also undergo financial reviews and more rigorous background investigations conducted through local field offices of the FBI.

The FBI reportedly has sent several agents to DOE in the last 10 years to try to improve the counterintelligence program, but has repeatedly been unsuccessful. A significant problem has been the lack of counterintelligence professionals, and a bureaucracy that "buried" them and left them without access to senior management or the Secretary of Energy. DOE's new



---

Counterintelligence Director now has direct access to the Secretary.

After traveling to the laboratories and interviewing counterintelligence officials, DOE's new Counterintelligence Director reported in November 1998:

*The counterintelligence program at DOE does not even meet minimal standards ... there is not a counterintelligence [program], nor has there been one at DOE [the Department of Energy] for many, many years. DOE's counterintelligence program requires additional training, funding, and accountability, according to this counterintelligence official. At present, an Office of Personnel Management contractor conducts DOE's background investigations. The new Director's opinion is that the present background investigations are "totally inadequate" and "do [not] do us any good whatsoever."*

Another problem area is that DOE's counterintelligence process presently does not have any mechanism for identifying or reviewing the thousands of foreign visitors and workers at the US national weapons laboratories. On one occasion reviewed by the Cox Committee, for example, scientists from a US National Laboratory met foreign counterparts in a Holiday Inn in Albuquerque, New Mexico, in order to circumvent their laboratory's security procedures.

One responsibility of DOE's new counterintelligence program would be to find out who visits the laboratories, including those from sensitive countries, what they work on while they visit, and whether their access is restricted to protect classified information. Mechanisms have been recommended to identify visitors and fully vet them. DOE will attempt to improve the database used for background checks.

Classified information has been placed on unclassified networks, with no system for either detection or reliable prevention. There are no intrusion detection devices to determine whether

hackers have attacked DOE's computer network. According to damage assessments reviewed by the Cox Committee, however, attacks on the computers at the US national weapons laboratories are a serious problem. E-mail is also a threat: the US national weapons laboratories cannot track who are communicating with whom. For example, over 250,000 unmonitored e-mails are sent out of the Sandia National Laboratory alone each week.

### **PRC Gains Sensitive Information from Hughes**

Hughes attempted to launch two communications satellites from the PRC on Long March rockets, which exploded before reaching orbit, one in 1992 and one in 1995. Allegations regarding technology transfer arose in connection with failure analysis investigations conducted by Hughes employees in the aftermath of these failed launches. Specifically, in 1992 and 1995, China Great Wall Industry Corporation launched two Hughes satellites manufactured for Australian (Optus B2) and Asian (Apstar 2) customers from a PRC launch facility in Xichang, PRC.

Both satellites were launched on a Long March 2E rocket. In both cases, an explosion occurred after take-off and before separation of the satellite. Hughes investigated the causes of both of these failed launches and determined that the rocket was the cause of the failures.

In the course of the investigations, Hughes communicated technical information regarding the rocket to the PRC that assisted the PRC in improving the Long March 2E rocket. The activities of Hughes employees in connection with the investigation of the failed launch in 1992 resulted in the transmission to the PRC of technical information that appears to have been approved by a US Government representative but not properly licensed. In the case of the 1995 Hughes failure investigation, Hughes employees exported technical information that also was approved by a US Government representative but should not have been authorized for export to the PRC.

---

In both cases, Hughes disclosed information to the PRC that related to improving the Long March 2E fairing, a portion of the rocket that protects the payload during launch. Such information was outside the scope of the original licenses Hughes obtained from the State and Commerce Departments, respectively, with respect to the export and launch of the Optus B2 and Apstar 2 satellites. Hughes claims that the 1993 Optus B2 failure analysis disclosures were cleared in advance by US Government officials, but neither Hughes nor the pertinent US Government agencies retained records that would substantiate this claim fully.

The lessons learned by the PRC from Hughes during the 1995 Apstar 2 failure investigation are directly applicable to fairings on other rockets, including those used to launch PRC military satellites.

Although the Long March 2E has not been used since 1995, it is possible that the PRC may have transferred the lessons learned from this launch failure investigation to its ballistic missile programs. These lessons could lead to the development of a more reliable fairing for use with advanced payloads on military ballistic missiles.

Hughes obtained a clearance for the 1995 disclosures that was improperly issued by a Commerce Department official. Hughes was confident that the cause of the 1992 launch failure on the PRC's Long March 2E rocket was the fairing. Hughes then ascertained with more certainty that the fairing was responsible for the 1995 launch failure. Hughes required that the PRC take appropriate corrective measures so that future launches of Hughes satellites on the Long March 2E rocket could occur and be insured.

Hughes employees conveyed to the PRC the engineering and design information necessary to identify and remedy the structural deficiencies of the fairing. At the time of the 1992 failure, the export of both the satellite and any information that might improve the rocket were subject to State Department licensing jurisdiction.

Hughes knew that the fairing was part of the rocket and that a State Department license was required to discuss improvements with the PRC. Although Hughes did not have a license to disclose information to the PRC relating to improvement of the fairing, Hughes, nonetheless, made such disclosures. Hughes claims that the Defense Technology Security Administration monitor authorized each disclosure. Contemporaneous Hughes records partially support this assertion. The monitor says he doubts that he in fact approved the disclosure, but says he cannot fully recall these matters.

Neither Hughes nor any relevant U.S. Government agency has been able to produce records substantiating all of the claimed approvals. Even if such approvals were in fact given, they would have exceeded the authority of the Defense Technology Security Administration monitor since he was not empowered to expand the scope of the license granted by the State Department. The monitor also should have known that a separate license was needed for the launch failure analysis activities. By the time of the 1995 failure investigation, partial jurisdiction for commercial satellites had been transferred to the Commerce Department, but licensing for improvements to any part of the rocket, such as the fairing, remained with the State Department.

Hughes officials who were responsible for the launch failure investigation in 1995 knew that technical information that would improve the rocket, including the fairing, was still subject to State Department jurisdiction and was not licensed for export. Nonetheless, Hughes sought Commerce Department approval to disclose information regarding the fairing to the PRC. A Commerce Department official, without consulting with Defense Department or State Department experts, approved that disclosure, he says, on the assumption that the fairing was part of the satellite, not the rocket. He now acknowledges that this decision was a mistake.

The Defense Department recently determined that the information Hughes made available to the PRC was sufficiently specific to inform the PRC of the kinds

---

of rocket changes and operational changes that would make the Long March 2E, and perhaps other rockets, more reliable. In particular, Hughes assisted the PRC in correcting the deficiencies in its models of the stresses or loads (such as buffeting and wind shear) that the rocket and payload experience during flight.

There are differing views within the US Government as to the extent to which the information that Hughes imparted to the PRC may assist the PRC in its ballistic missile development. There is agreement that any such improvement would pertain to reliability and not to range or accuracy. It is not clear, at present, whether the PRC will use a fairing that was improved as a result of Hughes' disclosures in a current or future ballistic missile program. Currently-deployed PRC ballistic missiles do not use fairings, and the PRC's future mobile land-based intercontinental ballistic missiles will probably not use a fairing. However, fairings are used by the PRC in launching military communications satellites and could be used for a submarine-launched ballistic missile.

In the opinion of the Cox Committee's independent expert, Dr. Alexander Flax, fairing improvements could also be of benefit to multiple independently-targeted reentry vehicle (MIRV) development, should the PRC decide to move in that direction.

Hughes also provided the PRC with practical insight into diagnostic and failure analysis techniques for identifying and isolating the cause of a launch failure. Whether or not the structural improvements to the fairing suggested by Hughes are of immediate use to the PRC's missile programs, that information expanded the PRC's repertoire of available technical solutions to future problems that it may encounter in its space and missile programs.

Finally, the Cox Committee's independent expert has concluded that Hughes provided the PRC with the benefit of its engineering experience and expertise. As a result, PRC engineers better understand how to conduct a failure analysis and how to design and

build more reliable fairings for rockets: "This will stand them in good stead in developing fairings (or shrouds) for ballistic missiles."

### **LORAL Investigation of Intelsat Launch Failure Provides PRC with Sensitive Information**

On February 15, 1996, a Long March 3B rocket carrying the US-built Intelsat 708 satellite crashed just after lift off from the PRC's Xichang launch center. This was the third launch failure in 38 months involving the PRC's Long March series of rockets carrying US-built satellite payloads. It also was the first commercial launch using the new Long March 3B. These events attracted intense attention from the international space launch insurance industry, and eventually led to a review of the PRC launch failure investigation by Western aerospace engineers.

The activities of the Western aerospace engineers who participated on the review team—The Independent Review Committee—sparked allegations of violations of US export control regulations. The review team was accused of performing an unlicensed defense service for the PRC that resulted in the improvement of the reliability of the PRC's military rockets and ballistic missiles.

The Intelsat 708 satellite was manufactured by Loral under contract to Intelsat, the world's largest commercial satellite communications services provider.

China Great Wall Industry Corporation, the PRC state-controlled missile, rocket, and launch provider, began an investigation into the launch failure. On February 27, 1996, China Great Wall Industry Corporation reported its determination that the Long March 3B launch failure was caused by a broken wire in the inner frame of the inertial measurement unit within the guidance system of the rocket. In March 1996, representatives of the space launch insurance industry insisted that

---

China Great Wall Industry Corporation arrange for an independent review of the PRC failure investigation.

In early April 1996, China Great Wall Industry Corporation invited Dr. Wah Lim, Loral's Senior Vice President and General Manager of Engineering and Manufacturing, to chair an Independent Review Committee that would review the PRC launch failure investigation. Lim then recruited experts to participate in the Independent Review Committee: four senior engineers from Loral, two from Hughes, one from Daimler-Benz Aerospace, and retired experts from Intelsat, British Aerospace, and General Dynamics.

The Independent Review Committee members and staff met with PRC engineers during meetings in Palo Alto, California, and in Beijing. During these meetings the PRC presented design details of the Long March 3B inertial measurement unit, and the committee reviewed the failure analysis performed by the PRC.

The Independent Review Committee took issue with the conclusions of the PRC investigation because the PRC failed to sufficiently explain the telemetry data obtained from the failed launch.

The Independent Review Committee members proceeded to generate a Preliminary Report, which was transmitted to China Great Wall Industry Corporation in May 1996 without prior review by any US Government authority. Before the Independent Review Committee's involvement, the PRC team had concluded that the most probable cause of the failure was the inner frame of the inertial measurement unit. The Independent Review Committee's draft report that was sent to the PRC pointed out that the failure could also be in two other places: the inertial measurement unit follow-up frame, or an open loop in the feedback path. The Independent Review Committee recommended that the PRC perform tests to prove or disprove all three scenarios.

After receiving the Independent Review Committee's report, the PRC engineers tested these

scenarios and, as a result, ruled out its original failure scenario. Instead, the PRC identified the follow-up frame as the source of the failure. The PRC final report identified the power amplifier in the follow-up frame to be the root cause of the failure.

According to the Department of Defense, the timeline and evidence suggests that the Independent Review Committee very likely led the PRC to discover the true failure of the Long March 3B guidance platform.

At the insistence of the State Department, both Loral and Hughes submitted "voluntary" disclosures documenting their involvement in the Independent Review Committee. In its disclosure, Loral stated that "Space Systems/Loral personnel were acting in good faith and that harm to US interests appears to have been minimal." Hughes' disclosure concluded that there was no unauthorized export as a result of the participation of Hughes employees in the Independent Review Committee.

Several US government offices, including the State Department, the Defense Technology Security Administration, the Defense Intelligence Agency, and other Defense Department agencies reviewed the materials, submitted by both Loral and Hughes in their disclosures to the State Department.

The Defense Department assessment concluded that "Loral and Hughes committed a serious export control violation by virtue of having performed a defense service without a license . . ."

The State Department referred the matter to the Department of Justice for possible criminal prosecution.

An interagency review team performed a review of the Independent Review Committee matter in 1998 to reconcile differences in the assessments of the other agencies. That interagency team concluded:

- The actual cause of the Long March 3B failure may have been discovered more quickly by

---

the PRC as a result of the Independent Review Committee report

- Advice given to the PRC by the Independent Review Committee could reinforce or add vigor to the PRC's design and test practices
- The Independent Review Committee's advice could improve the reliability of the PRC's rockets
- The technical issue of greatest concern was the exposure of the PRC to Western diagnostic processes, which could lead to improvements in reliability for all PRC missile and rocket programs

### **PRC Targeting of Advanced Machine Tools**

The PRC is committed to the acquisition of Western machine tool technology, and the advanced computer controls that provide the foundation for an advanced aerospace industry. Although the PRC acquires machine tools from foreign sources in connection with commercial ventures, it also seeks foreign-made machine tools on a case-by-case basis to support its military armament programs.

Moreover, the proliferation of joint ventures and other commercial endeavors that involve the transfer or sale of machine tools to the PRC makes it more difficult for foreign governments and private industry to distinguish between civilian and military end-uses of the equipment.

CATIC's purchase of used machine tools from McDonnell Douglas, now part of Boeing, is one illustration of the complexities and uncertainties faced by private industry and the US Government in these endeavors.

Machine tools are essential to commercial industry, and high precision, multiple-axis machine tools broaden the range of design solutions for weapon components and structural assemblies. Parts and structures can be designed with advantages in weight and cost relative to what could be achieved

with less advanced machine tools. For military and aerospace applications, the level of manufacturing technology possessed by a country directly affects the level of military hardware that can be produced, and the cost and reliability of the hardware.<sup>94</sup>

### **Case Study: McDonnell Douglas Machine Tools**

The Cox Committee determined that the US Government was generally unaware of the extent to which the PRC has acquired machine tools for commercial applications and then diverted them to military end uses. The McDonnell Douglas case illustrates that the PRC will attempt diversions when it suits its interests.

At the request of Congress, the US GAO in March 1996 initiated a review of the facts and circumstances pertaining to the 1994 sale of McDonnell Douglas machine tools to CATIC. The GAO issued its report on November 19, 1996. The report can be summarized as follows:

- In 1992, McDonnell Douglas and CATIC agreed to co-produce 20 MD-82 and 20 MD-90 commercial aircraft in the PRC. Known as the Trunkliner Program, the aircraft were to serve the PRC's domestic "trunk" routes. In late 1994, a contract revision reduced the number of aircraft to be built in the PRC to 20, and added the purchase of 20 US-built aircraft.
- CATIC is the principal purchasing arm of the PRC's military as well as many commercial aviation entities. Four PRC factories, under the direction of AVIC and CATIC, were to be involved in the Trunkliner Program.
- In late 1993, CATIC agreed to purchase machine tools and other equipment from a McDonnell Douglas plant in Columbus, Ohio that was closing. The plant had produced parts for the C-17 transport, the B-1 bomber, and the Peacekeeper missile. CATIC also purchased four additional machine tools from McDonnell Douglas that were located at Monitor Aerospace



---

Corporation in Amityville, New York, a McDonnell Douglas subcontractor.

- The machine tools were purchased by CATIC for use at the CATIC Machining Center in Beijing—a PRC-owned facility that had yet to be built—and were to be wholly dedicated to the production of Trunkliner aircraft and related work. McDonnell Douglas informed the US Government that CATIC would begin construction of the machining center in October 1994, with production to commence in December 1995.
- In May 1994, McDonnell Douglas submitted license applications for exporting the machine tools to the PRC and asked that the Commerce Department approve the applications quickly so that it could export the machine tools to the PRC, where they could be stored at CATIC's expense until the machining facility was completed. Following a lengthy interagency review, the Commerce Department approved the license applications on September 14, 1994, with numerous conditions designed to mitigate the risk of diversion.
- During the review period, concerns were raised about the possible diversion of the equipment to support PRC military production, the reliability of the end user, and the capabilities of the equipment being exported. The Departments of Commerce, State, Energy, and Defense, and the Arms Control and Disarmament Agency, agreed on the final decision to approve these applications.
- Six of the machine tools were subsequently diverted to Nanchang Aircraft Company, a PRC facility engaged in military and civilian production over 800 miles south of Beijing. This diversion was contrary to key conditions in the licenses, which required the equipment to be used for the Trunkliner program and to be stored in one location until the CATIC Machining Center was built.

- Six weeks after the reported diversion, the Commerce Department suspended licenses for the four machine tools at Monitor Aerospace in New York that had not yet been shipped to the PRC. Commerce subsequently denied McDonnell Douglas's request to allow the diverted machine tools to remain in the unauthorized location for use in civilian production. The Commerce Department approved the transfer of the machine tools to Shanghai Aviation Industrial Corporation, a facility responsible for final assembly of Trunkliner aircraft. The diverted equipment was relocated to that facility before it could be misused.
- The Commerce Department did not formally investigate the export control violations until six months after they were first reported. The US Customs Service and the Commerce Department's Office of Export Enforcement are now conducting a criminal investigation under the direction of the Department of Justice.<sup>95</sup>

### **PRC Targeting of US Jet Engines and Production Technology**

The PRC's acquisition of aerospace and defense industrial machine tools from US and foreign sources has expanded its manufacturing capacity and enhanced the quality of military and civilian commodities that the PRC can produce.<sup>96</sup> These acquisitions will support the PRC's achievement of a key goal: the development of an aerospace industrial base that is capable of producing components and structural assemblies for modern manned aircraft and cruise missiles.<sup>97</sup>

In the mid-1980s and early 1990s, the PRC apparently adopted a three-track approach to acquiring US equipment and technologies in order to advance its own military jet engine capabilities:

- The diversion of engines from commercial end uses
- Direct purchase
- Joint ventures for engine production

---

The PRC's acquisition targets suggest that it planned to acquire several families of jet engines that could be adapted to various military and commercial applications.<sup>98</sup>

In 1983, the PRC legally acquired two General Electric (GE) CFM-56 jet engines, ostensibly to analyze the engines for a potential civil aircraft upgrade program. In the course of the export licensing process, the Defense Department insisted on restricting the PRC's use of the engines. Under the terms of the licensing agreement:

*No technical data was to be transferred with the engines; the Chinese were not to disassemble the engines; and finally, if the Trident [civil aircraft] retrofit program had not begun within 1 year of the engines' arrival, the engines were to be repurchased by the manufacturer. In addition, the Chinese offered to retrofit engines at a Shanghai commercial aircraft facility where GE personnel would be able to monitor Chinese progress.*<sup>99</sup>

Defense Department officials were concerned because the CFM-56 hot sections are identical to those used in the engines that power the US F-16 and B-1B military aircraft.<sup>100</sup>

The PRC later claimed that the CFM-56 engines were destroyed in a fire.<sup>101</sup> More likely, however, is that the PRC violated the US end-use conditions by reverse engineering part of the CFM-56 to develop a variant for use in combat aircraft.<sup>102</sup>

Despite the suspected reverse engineering of the two GE jet engines that were exported in 1983, GE reportedly signed a contract in March 1991 with the Shenyang Aero-Engine Corporation for the manufacture of parts for CFM-56 engines.<sup>103</sup> According to one source, Shenyang "put in place quality and advanced manufacturing systems to meet US airworthiness standards."<sup>104</sup>

The PRC aggressively attempted to illegally acquire GE's F404 engine, which powers the US F-18 fighter.<sup>105</sup> The PRC likely intended to use the F404 jet engine in its F-8 fighter.<sup>106</sup> The PRC

succeeded in acquiring some F404 technology through an indirect route by purchasing the LM-2500, a commercial GE gas turbine containing the F404 hot section.<sup>107</sup>

In addition, GE has reportedly proposed a joint venture with the PRC to manufacture the so-called CFM-56-Lite. The engine could power the PRC's planned AE-100 transport.<sup>108</sup>

The PRC also has targeted large engines for aerospace and non-aerospace applications. The PRC's acquisition plans reportedly include Pratt & Whitney JT-8 series engines and technology to support its large aircraft projects, as well as marine derivatives of the GE LM-2500 for naval turbine propulsion projects.<sup>109</sup> Regarding the JT-8 series:

In August 1986, CATIC licensed the technology for the US Pratt and Whitney FT8 gas turbine engine, including joint development, production and international marketing rights. The FT8 is a development of the JT8D-219 aero-engine (used to power Boeing 727, Boeing 737, and MD-82 aircraft), and can produce 24,000 kW (33,000 hp). (It) represented another significant technical leap for China's gas turbine capability . . . Chinese students were also sponsored by Pratt and Whitney for graduate level aerospace training in the United States.<sup>110</sup>

The PRC's efforts to acquire compact jet engines can be traced to 1965, when the Beijing Institute of Aeronautics and Astronautics launched a project to copy the US Teledyne-Ryan CAE J69-T-41A.<sup>111</sup>

The Teledyne engine powered the US Air Force AQM-34N Firebee reconnaissance drone, a number of which were shot down over the PRC during the Vietnam conflict.<sup>112</sup> The PRC's copy of the US turbojet, dubbed WP-11, began ground testing in 1971 and currently powers the PLA's HY-4 "Sadsack," a short-range anti-ship cruise missile.<sup>113</sup>

The PRC began work on cruise missile engines in the 1980s. The PRC's interest in developing long-range cruise missiles increased dramatically after

---

the 1991 Persian Gulf War, when the performance of US Tomahawk cruise missiles demonstrated the effectiveness of precision missile strikes using conventional warheads. However, technical challenges slowed Beijing's efforts. For this reason, the PRC has attempted to acquire foreign-built engines for technical exploitation. If the PRC succeeds in building cruise missile propulsion and guidance systems, then it would probably not have difficulty marketing cruise missiles to third world countries.<sup>114</sup>

In 1990, the PRC attempted to advance its cruise missile program by purchasing the Williams FJ44 civil jet engine.<sup>115</sup> This compact turbofan was derived from the engine that powers the US Tomahawk cruise missile. The FJ44 engine might have been immensely valuable to the PRC for technical exploitation and even direct cruise missile applications.<sup>116</sup> But the PRC's effort to acquire FJ44 engines was rebuffed.<sup>117</sup>

### **Case Study: Garrett Engines**

The redundancy inherent in the PRC's three-track approach to advancing its military jet engine capabilities—diversion of engines from commercial use, direct purchase, and joint ventures—began to bear fruit in the early 1990s.<sup>118</sup>

The Cold War's end and a liberalization of Cold War-era export controls on dual-use products and technologies opened new opportunities for the PRC to acquire advanced jet engines and production capabilities. A notable opportunity developed in 1991 when, as part of an overall liberalization of export controls by the Coordinating Committee for Multilateral Export Controls (COCOM), the Commerce Department decontrolled a popular jet engine manufactured by Allied Signal's Garrett Engine Division.

Prior to 1991, the Garrett engine required an individual validated license that included restrictive conditions.

The Commerce Department's decision that Garrett jet engines were decontrolled ensured that they could be exported to the PRC without a license or US Government review. The decision also opened the way for a jet engine co-production arrangement sought by the PRC.

Negotiations for a co-production deal between Allied Signal and PRC officials progressed until July 1992, when the Defense Department learned of the plan.<sup>119</sup> The Defense Department's reaction to the news sparked an interagency review of the Commerce Department's decision to decontrol the Garrett engines.

The co-production deal was terminated after the review demonstrated the potential national security implications of transferring jet engine production capabilities to the PRC.<sup>120</sup>

### **PRC Targeting of Garrett Engines**

The PRC's reported motivation for initiating the Garrett engine purchase was the PRC's requirement for a reliable, high-performance Western engine for its developmental K-8 military aircraft.<sup>121</sup>

PRC aerospace organizations involved in the project included:

- CATIC
- China Nanchang Aircraft Manufacturing Company
- China National South Aero-Engine and Machinery Company.<sup>122</sup>

The PRC's access to the Garrett TFE-731 may have influenced its choice of small jet engines in general, and K-8 propulsion in particular. The PLA purchased a fleet of Learjets from the US on the understanding that the aircraft would be for civil use. It is suspected, however, that the PLA diverted both the aircraft and the engines for military purposes, including PLA reconnaissance missions.<sup>123</sup>

---

## US Government Approval of the Initial Garrett Engine Exports

In August 1989, Allied Signal applied for an export license to sell a variant of the TFE-731, the TFE-731-2A-2A, to the PRC. Four engines and spare parts were to be shipped.<sup>124</sup> The US Federal Aviation Administration (FAA) had certified the TFE-731-2A-2A as a “civil” engine.<sup>125</sup>

According to Iain S. Baird, then-Deputy Assistant Secretary of Commerce for Export Administration, the Commerce Department had licensing authority for the civil engine regardless of its military (i.e., the PLA’s K-8 military aircraft) application.<sup>126</sup>

The 1989 application for the export of the Garrett engines to the PRC raised concerns among officials at the Defense Technology Security Administration, which was the focal point for export policy guidance and license reviews within the Defense Department.<sup>127</sup>

Given this Defense Department judgment, a condition was placed by the Commerce Department on the export license for the TFE-731-2A-2As:

*“There is to be no transfer of engine design or manufacturing technical data provided with this transaction.” [Emphasis added]*<sup>128</sup>

COCOM also reviewed the case. Subsequently, the Commerce Department issued an Individual Validated License (number D032648) for the Garrett engines on May 30, 1990.<sup>129</sup>

In December 1990, Allied Signal asked the Commerce Department for approval to sell an additional 15 of the TFE-731-2A-2A engines to the PRC.<sup>130</sup>

These engines were reportedly to be used for the first production run of the PLA’s K-8 military aircraft, which were to be sold to Pakistan. The Defense Department and COCOM again reviewed the license application, and Defense requested conditions that would forbid the release of TFE-731-2A-2A “design methodology, hot section

repair/overhaul procedures and manufacturing information.”<sup>131</sup>

On June 12, 1991, the Commerce Department granted Individual Validated License D130990, which included the Defense Department’s recommended conditions.<sup>132</sup>

## Commerce Department Decontrol of the Garrett Jet Engines

In August 1991, Allied Signal requested that the FAA re-certify the TFE-731-2A-2A engine with a digital electronic engine controller.<sup>133</sup> The FAA had certified the engine in 1988 with an analog engine controller.<sup>134</sup>

It is unclear from the available information whether the PRC requested this upgrade of the engine to include the digital electronic engine controller, or whether Allied Signal decided to upgrade the engine on its own initiative.<sup>135</sup>

On September 1, 1991, the Commerce Department published revisions to the Export Administration Regulations to reflect liberalized export controls that had been agreed to by the United States and its COCOM partners.<sup>136</sup> The revised regulations decontrolled many jet engines, but continued to control exports of engines equipped with full authority digital engine control (FADEC) systems.<sup>137</sup>

These militarily sensitive systems control jet engine operations to permit, among other things, maximum propulsion performance for manned and unmanned military air vehicles.<sup>138</sup>

According to Defense Department records, Allied Signal sent a one-page document to the Commerce Department on September 30, 1991 representing that the TFE-731-2A-2A did not use a FADEC system, but instead used a less capable digital electronic engine controller (DEEC). For this reason, Allied Signal officials believed the TFE-731-2A-2A was completely decontrolled under the revised Export Administration Regulations and COCOM controls.<sup>139</sup>

---

Technical experts at the Defense Technical Security Agency had already presented their analysis to Commerce Department officials, countering that the TFE-731-2A-2A contained a FADEC and therefore remained controlled under COCOM and US regulations.<sup>140</sup>

On October 1, 1991, one day after receiving the Allied Signal document regarding the FADEC issue, the Commerce Department ruled that the TFE-731-2A-2A did not contain a FADEC. The Commerce Department then informed Allied Signal's Garrett Engine Division that it could export TFE-731-2A-2A jet engines to the PRC under a General License (a so-called G-DEST license) pursuant to the Export Administration Regulations, as long as production technology was not transferred.<sup>141</sup>

Defense Department records indicate that officials at the Defense Technology Security Administration concurred with the Commerce Department decision to permit this export, but mistakenly believed it was still under an Individual Validated License arrangement - that is, with the requested Defense Department conditions.<sup>142</sup>

Subsequently, the Commerce Department amended the October 1, 1991 decision and notified Allied Signal on November 25, 1991 that it had decontrolled the TFE-731-2A-2A entirely.<sup>143</sup>

Engine production technology could now be exported to the PRC without a license.<sup>144</sup> According to Defense Department records, Commerce Department officials relied exclusively on Allied Signal's September 30, 1991 representation concerning the engine controller for the TFE-731-2A-2A - that is, that the controller was not a FADEC, and thus was no longer controlled.<sup>145</sup>

Bruce C. Webb, then a senior analyst at the Commerce Department's Office of Nuclear Controls, recalls that a US Government advisory group had reviewed the Allied Signal document and agreed with the company's assertion that the TFE-731-2A-2A was not equipped with an embargoed

FADEC.<sup>146</sup> However, in response to document requests by the Select Committee, the Commerce Department was unable to provide any records of any technical reviews that it may have conducted.<sup>147</sup>

### **The Interagency Review of the Proposed Export of Garrett Engines**

Iain Baird, then-Deputy Assistant Secretary of Commerce for Export Administration, claims that the Commerce Department coordinated with appropriate agencies before making the General License determination in November 1991. However, the Commerce Department was unable to provide the Select Committee with any documentary evidence to this effect.<sup>148</sup>

A Defense Technology Security Administration staff member suggests that other agencies learned of the decision by chance, or "dumb luck." In addition, according to a December 29, 1992 Defense Department memorandum for the record:

*Commerce approved, with DoD and COCOM concurrence, the sale of 15 Garrett TFE-731-2A-2A engines to the PRC for incorporation into military trainers being exported to Pakistan.*

In July 1992 DTSA [the Defense Technology Security Administration] learned from cable traffic that the PRC and Garrett were negotiating an arrangement to co-produce this engine in China for use in PLA military trainers.

We learned shortly thereafter that Department of Commerce had determined in November 1991 that the engine did not require an Individual Validated License (IVL) for shipment to the PRC.

Department of Commerce, without consulting with Department of Defense, classified the engine and technology decontrolled (or "G-DEST") under the COCOM Core List implemented on 1 September 1991.

DTSA believes the export requires an IVL [Individual Validated License].<sup>149</sup>



After receiving a copy of the July 1992 cable, the Defense Technology Security Administration initiated an interagency review of the Commerce Department General License decision regarding the Garrett engines.<sup>150</sup> The Commerce Department agreed to suspend its decision pending the outcome of the review.

Officials at the Defense Technology Security Administration reportedly were especially concerned over any transfer of jet engine production technology to the PRC. They were also surprised that the Commerce Department opted not to coordinate its decision, given the agency's oft-repeated concerns over any transfer of jet engine production technology to the PRC.<sup>151</sup>

The Commerce Department's decision to decontrol Garrett engine technology was considered in the context of several US policies. Two policies in particular dominated the interagency debate: the 1991 Enhanced Proliferation Control Initiative (EPCI), and COCOM controls on jet engine technologies.

### **Consideration of Enhanced Proliferation Control Initiative Regulations**

The Enhanced Proliferation Control Initiative was established by the Bush administration to provide a non-proliferation "safety net." It was intended to restrict the export of technologies usable for chemical and biological weapons or missiles, regardless of whether such technologies were controlled under existing international agreements (for example, under the 1987 Missile Technology Control Regime).

As explained by the Commerce Department:

*Foreign policy controls are being imposed on certain exports by adopting a policy of denial for items that already require a validated license, for any reason other than short supply, where the export is determined to be for a facility involved in the development, production, stockpiling, delivery, or use of chemical or biological weapons or of missiles.*

*The purpose of these controls is to prevent American contribution to, and thereby distance the United States from, the proliferation of chemical and biological weapons and missile development.*

*These controls serve to demonstrate US opposition to the spread of these weapons and provide specific regulatory authority to control exports from the United States of commodities or technology where there is a significant risk that they will be used for these purposes. [Emphasis added]<sup>152</sup>*

According to the August 1991 interim Enhanced Proliferation Control Initiative regulations, the Commerce Department should have conducted a "case-by-case" review of Allied Signal's proposed export to determine whether it "would make a material contribution to the proliferation of missiles." If the export were "deemed to make such a contribution, the license [would] be denied."<sup>153</sup>

Baird states that an Enhanced Proliferation Control Initiative review was not conducted for the engines, but was conducted for the production technology: "As far as the engines went, sending the whole engine up, we didn't feel it raised EPCI concerns. As far as the technology went, we did." Baird did not further explain the basis for the Commerce Department decision that the Garrett engines themselves did not require an Enhanced Proliferation Control Initiative review; nor did he explain why the technology did raise EPCI concerns.<sup>154</sup>

The Department of Commerce was unable to provide the Select Committee with any records of the Enhanced Proliferation Control Initiative review it conducted for the Garrett engine production technology.<sup>155</sup>

Allied Signal's partners in the Garrett engine transaction included:

- CATIC
- China Nanchang Aircraft Manufacturing Company

- 
- The China National South Aero-Engine and Machinery Company

A 1992 US Government review of these proposed end users found that the export of Garrett engine production technology to the PRC could pose a national security threat to the United States.

The review found that PRC co-production of Garrett TFE-731-2 engines would enable Beijing to develop higher quality turbojet and turbofan engines for use in military and civilian aircraft and in cruise missiles. PRC access to this production process would also give Beijing the means to extend the range of its cruise missiles. This was of special concern because PLA missiles, rockets, and aircraft are produced at facilities also used for civilian production.

A Garrett representative confirmed that the Zhuzhou South Motive Power and Machinery Complex was the intended producer of the Garrett TFE-731-2 engine. There was concern that a flow-through of applicable production technologies to the PRC's cruise missile engine program was almost inevitable.<sup>156</sup>

A copy of a US turbojet engine reportedly now powers the PLA's HY-4 cruise missile.<sup>157</sup> In addition, the conditions placed on the export of the Garrett engine technology of course would not prevent the PRC from reverse engineering the engine if that were the PRC's intent.<sup>158</sup>

Each of the PRC participants in the Garrett engine co-production venture produces military hardware. Despite the assurances of Allied Signal that the engines it proposed to produce in the PRC would be used entirely for commercial purposes, PLA personnel were prominent in the negotiations with Garrett. The CATIC representatives were the same individuals who were prominent in the Committee on Foreign Investment in the United States (CFIUS) case involving the attempted purchase of MAMCO, a Boeing contractor, by CATIC. This is the only CFIUS case in which the President reversed a sale on national security grounds.<sup>159</sup>

Because the PRC could incorporate complete TFE-731-2A-2A engines or modified variants directly into cruise missile airframes, export to the PRC of the engines themselves - as well as the production technology - presented a national security threat.<sup>160</sup>

### **Consideration of COCOM and Export Administration Regulations**

COCOM and Export Administration Regulation reviews were conducted to assess sensitive components in the Garrett TFE-731-2A-2A jet engine.

When Allied Signal's Garrett Engine Division upgraded the TFE-731-2A-2A with the addition of a digital engine controller, it claimed that the new system did not require an export license under the revised Export Administration Regulations and COCOM controls. It was determined that COCOM had not developed an agreed-upon technical definition to distinguish restricted from unrestricted engine controllers.<sup>161</sup> This shortfall in the regime set the stage for an extended interagency debate over the status of the TFE-731-2A-2A vis-à-vis COCOM regulations.

The Defense Department believed the Garrett engines contained an embargoed, full authority digital engine control (FADEC) system. Moreover, the Defense Department obtained new information about improvements to the Garrett TFE-731-2A-2A that raised additional national security concerns.<sup>162</sup>

Regarding the FADEC issue, the Defense Department acquired analysis and technical studies from numerous sources. A Defense Technology Security Administration analysis explained, for example:

The Garrett engine contains what [Allied Signal] calls a Digital Electronic Engine Control (DEEC) but describes in company literature as "full-authority, automatic engine control." DTSA maintains that the DEEC is a FADEC for the following reasons:

---

*FAA certification officials state in writing that the “DEEC” controller is a FADEC. Also DoD experts at the Air Force Aeronautical Systems Center and the Naval Air Warfare Center have assessed that the Garrett engine controller is a FADEC.*<sup>163</sup>

Additional confirmation of these findings was contained in a technical paper developed by the engineering staff at the Defense Technology Security Administration:

In summary, the entire DoD Category 9 [aero-engines] negotiating team to COCOM during 1990-91 . . . are in agreement after detailed analysis, with assistance from experts in controls from Navy, Air Force and FAA, of data proprietary to Allied-Signal and otherwise, that the ASCA [Allied Signal Controls & Accessories division] DEEC, P/N 2118002-202 is a FADEC.

Allied-Signal’s memo to DTSA . . . shows this is indeed the FADEC utilized on the GED [Garrett Engine Division] TFE731-2A-2A engine.

The Defense Department inquiry found further that Allied Signal initially did not provide accurate information to the FAA during the civil certification process for the TFE-731-2A-2A:

*FAA engineers rebuked GED [Garrett] in 1988 for their claim that the -2A engine was a direct derivation from a -2 engine rather than being derived from a TFE731-3. GED subsequently provided FAA with a corrected derivation showing that the engine was actually a TFE731-3 with TFE-731-3B parts and components rather than TFE731-2 components.*

*Substantial improvement to the TFE731-2A engine occurred when the so-called “Extended Life Turbine Modifications” were added during December, 1991, only one month after DOC [Commerce] had notified GED it had decontrolled the engine.*

*The Extended Life Turbine (ELT) resulted from the NASA program to obtain significant reductions in noise and emission levels, i.e., decreased infrared (IR) signature. The ELT has an enhanced damage tolerance and changes TFE731-series engines from an expected life of approximately 6,000 hours to 10,000 hours.*

In summary, the engine GED [Garrett] submitted for a ‘paper certification’ as a TFE731-2A in 1988 was not a derivative of a -2 engine but was derived from a TFE731-3 with a TFE731-3B LP compressor. The changes noted above were included in the 1988 engine, i.e., the A5 seal and both LP compressor and turbine blades changed. The ELT was added in 1991.

In conjunction with the slight derating of the engine in 1988, life expectancy of this engine is greatly enhanced over a TFE731-3 turbofan engine; it is more durable, reliable, and generally more appropriate for use on military aircraft.

No applications of this engine to civil airframes are known to have been attempted by Allied-Signal, only military.<sup>164</sup> [Emphasis added]

The evidence obtained by the Defense Department indicated that the TFE-731-2A-2A was not simply a 20-year old engine for business jets, as Allied Signal and Commerce Department officials had claimed.<sup>165</sup> (Indeed, as of January 3, 1999, the TFE-731-2A-2A has never been used in a business jet.)<sup>166</sup>

It is true that the engine had been derived from the TFE-731-3, an engine used in both civil and military applications, including the Cessna Citation III business jet and the CASA C-101BB ground-attack jet. But the engine had been upgraded with a new turbine to lower its infrared signature, thus improving the combat survivability of the aircraft in which it would be contained - for example, through the ability to escape detection by surface-to-air missiles.<sup>167</sup>

---

## Resolution of the Garrett Engine Controversy

The Garrett engine controversy was ultimately resolved through an interagency agreement at the Deputy Assistant Secretary level. Regarding the disputed engine controller, the Deputy Assistant Secretary of Defense for Counterproliferation Policy, Mitchel B. Wallerstein, described an interagency compromise in a March 21, 1994 letter to the Deputy Assistant Secretary for Export Controls at the State Department:

Defense is prepared to agree with the Allied (and Commerce) determination that the engine does not include a Full Authority Digital Engine Control System (FADEC) which meets the IVL [Individual Validated License] criteria. With respect to the 2A-2A engine, our proposed carve out from the definition of FADEC would provide a basis for a Commerce G-DEST classification, which would allow sales of the 2A-2A engine to the PRC, including its military, without prior [US Government] review and approval. It is unclear whether such a definitional carve out would require multilateral coordination with our current allies before such a G-DEST classification is made.<sup>168</sup>

The State Department agreed with this proposal, and stated further: “We do not believe that it is necessary to coordinate multilaterally with our COCOM partners before moving to G-DEST treatment.”<sup>169</sup>

Peter M. Leitner, senior trade advisor at the Defense Technology Security Administration, believes that the “definitional carve out” entailed a political decision to change the definition of the engine controller in order to circumvent export regulations and, in this case, avoid a COCOM review. According to Leitner, “you come up with some unique definition of the item and try to exempt or carve out coverage of that item in the regulations.”<sup>170</sup>

Baird believes that COCOM reviewed the export license application for the upgraded variant of the Garrett TFE-731-2A-2A.<sup>171</sup> Webb believes

COCOM did not review the application.<sup>172</sup> The Commerce Department was unable to provide records of any COCOM review conducted for the upgraded Garrett engines.<sup>173</sup>

Defense Department records indicate that some US government officials believed a COCOM review of the upgraded engines was essential. Without such a review, the United States might be seen by its partners as attempting to “circumvent CoCom controls.”<sup>174</sup>

Wallerstein interprets the reference to “a carve out from the definition of FADEC” to mean that the disputed FADEC engine controller would be removed or modified to ensure that the TFE-731-2A-2A could be exported without controlled technology.<sup>175</sup> However, Wallerstein does not recall seeing any technical proposal from Allied Signal to modify the engine controller.<sup>176</sup>

The documentary record suggests that the final, upgraded variant of the Garrett TFE-731-2A-2A was never submitted for a review by COCOM, which ceased operations in April 1994.<sup>177</sup>

The status of the Garrett engines vis-à-vis the Enhanced Proliferation Control Initiative was largely resolved on August 19, 1993 during a meeting of the Commerce Department-chaired Operating Committee on Export Policy. According to a record of the meeting:

*Commerce, State and Defense have agreed to treat these commodities as if they were controlled. Moreover, [Allied Signal] has agreed not to transfer any co-production technology relating to these engines to the PRC.*<sup>178</sup>

This interagency decision was finalized and reported in the news media in October 1995. As the Wall Street Journal reported then:

*Allied Signal already has shipped about 40 built-up engines to China under the liberalized post-Cold War export rules, and isn't being deterred from exporting 18 more that the Chinese have ordered.*



But when it sounded out the US Commerce Department last summer about its coproduction plan, the company was told that if it formally applied for a license to do so the application would be denied under the rules of the Enhanced Proliferation Control Initiative. The company decided not to apply for the license.<sup>179</sup>

Between 1992 and 1996, Allied Signal reportedly exported 59 of these TFE-731-2A-2A jet engines to the PRC. Beijing's main interest was in acquiring a production capability for the engines; thus, it halted further orders when co-production plans were scuttled.<sup>180</sup>

### **The PRC Continues to Acquire Jet Engine Production Processes**

The PRC is continuing its effort to acquire production processes for US jet engines. For example, Pratt & Whitney Canada, a subsidiary of Connecticut-based United Technologies, in February 1996 became "the first foreign company to establish an aviation parts manufacturing joint venture in China (with Chengdu Engine Company)."<sup>181</sup> The Chengdu Engine Company manufactures components for, among other purposes, large jet engines used in Boeing aircraft.<sup>182</sup> The Chengdu factory also manufactures parts for the PRC's WP13 turbojet engine, which powers the PLA's F-8 fighter.<sup>183</sup> In 1997, a new joint venture was reportedly proposed for Chengdu.

A consortium of Pratt and Whitney, Northrop Grumman and Hispano-Suiza are offering a new aero-engine, the PW6000, specifically designed to power the AE-100 transport, and are planning to establish an aero-engine joint venture at Chengdu, Sichuan Province.<sup>184</sup>

United Technologies operates additional aviation joint ventures with Xi'an Airfoil Technology Company and China National South Aero-Engine and Machinery Company. These ventures are largely comprised of manufacturing jet engine "cold section" components or producing relatively low-technology "hot section" components.<sup>185</sup>

### **Endnotes**

<sup>1</sup> Testimony of Nicholas Eftimiades, October 15, 1998.

<sup>2</sup> Interview of James Lilley, November 17, 1998.

<sup>3</sup> Deng Xiaoping died 19 February 1997.

<sup>4</sup> For the official report on this program, see "Decade-Long Hi-Tech Program Bears Fruit," Xinhua News Agency, September 27, 1996.

<sup>5</sup> Su Kuoshan, "Road of Hope-Reviewing the Accomplishment of the '863' Project on the 10th Anniversary of its Implementation," Jiefangjun Bao, April 5, 1996, reproduced in Foreign Broadcast Information Service, Daily Report, May 8, 1996, FBIS-CHI-96-089.

<sup>6</sup> Major Mark Stokes, "China's Strategic Modernization: Implications for US National Security," USAF Institute for National Security Studies, July 1998.

<sup>7</sup> Cui Ning, "Hi-Tech Projects Highlight Five Areas," China Daily, April 3, 1996; in FBIS. See also Ding Hengngao, COSTIND Director, speech delivered on March 28, 1996, "Review of the 863 Plan over the Past Ten Years"; Stokes.

<sup>8</sup> These individuals often jump many bureaucratic levels to take their positions. Tai Ming Cheung, See, e.g., "China's Princelings," Kim Eng Securities, January 1995; Murray Scot Tanner and Michael Feder, "Family Politics, Elite Recruitment, and Succession in Post-Mao China," Australian Journal of Chinese Affairs, July 1993.

<sup>9</sup> Interview of James Mulvenon, October 16, 1998.

<sup>10</sup> See Murray Scot Tanner and Michael Feder, "Family Politics, Elite Recruitment, and Succession in Post-Mao China," Australian Journal of Chinese Affairs, July 1993.

<sup>11</sup> James Mulvenon, "Chinese Military Commerce and US National Security," RAND, July 1997; David Jackson, "US Probes Whether Beijing Gave Money to Influence Policy," Chicago Tribune, February 14, 1997.

<sup>12</sup> Ibid.

<sup>13</sup> Tracy Connor, "New Asiagate Figure Has Military History," New York Post, November 7, 1998.

<sup>14</sup> Interim Report of the House Government Reform and Oversight Committee ("HGROC Report") Chapter IV C.

<sup>15</sup> Deposition of Shen Jun before the Select Committee (Dec. 8, 1998); Japanese Firms Buy Into Satellite Telephone Co., Information Access Newsbytes (July 9, 1996).

<sup>16</sup> See generally, "Liu's Deals with Chung: An Intercontinental Puzzle," David Jackson and Lena H. Sun, *Washington Post*, May 24, 1998.

<sup>17</sup> Interim Report of the House Government Reform and Oversight Committee ("HGROC Report") Chapter IV C.

<sup>18</sup> Ibid.

<sup>19</sup> Ibid.

<sup>20</sup> Ibid.



---

<sup>21</sup> “Red Face Over China; Did a Chinese plot persuade Clinton to let a US company give China its rocket science? No. Politics (and policy) did,” Eric Pooley et. al., *Time*, June 1, 1998.

<sup>22</sup> Interim Report of the House Government Reform and Oversight Committee (“HGROC Report”) Chapter IV C. “Liu’s Deals with Chung: An Intercontinental Puzzle,” David Jackson and Lena H. Sun, *Washington Post*, May 24, 1998.

<sup>23</sup> Testimony of James Mulvenon, RAND, before the Select Committee (Oct. 15, 1998); John Frankenstein and Bates Gill, “Current and Future Challenges Facing Chinese Defense Industries,” *China Quarterly* (June 1996).

<sup>24</sup> Bates Gill and Taeho Kim, “China’s Arms Acquisitions from Abroad, A Quest for Superb and Secret Weapons,” Stockholm International Peace Institute, Oxford University Press, 1995.

<sup>25</sup> *Ibid.*

<sup>26</sup> Shawn L. Twing, “Congress Calls for Sanctions if Israeli Technology Transfer to China is Proven,” *The Washington Report*, November/December 1996. See also Bates Gill and Taeho Kim, “China’s Arms Acquisitions from Abroad, A Quest for Superb and Secret Weapons,” Stockholm International Peace Institute, Oxford University Press, 1995; Tony Capaccio, “Israeli Arms Transfers of US Technology Remain and Abrasive Issue,” *Defense Week*, June 5, 1995.

<sup>27</sup> “The National Security Science and Technology Strategy,” US Office of Science and Technology Policy, 1996.

<sup>28</sup> Kathleen Walsh, “US Technology Transfers to the People’s Republic of China,” DFI International, December, 1997.

<sup>29</sup> Paul Blustein, “China Plays Rough: Invest and Transfer Technology, or No Market Access,” *Washington Post*, October 25, 1997.

<sup>30</sup> Kathleen Walsh, December, 1997.

<sup>31</sup> Walsh, December, 1997, (stating the United States is “somewhere in the middle” among countries in its willingness to transfer technology).

<sup>32</sup> Testimony of Nicholas Eftimiades, October 15, 1998.

<sup>33</sup> See “Challenges and Opportunities for US Businesses in China,” testimony of JayEtta Hecker, GAO, before the Committee on Banking and Financial Services, US House of Representatives, July 29, 1996.

<sup>34</sup> Interview of John Foorde, September 23, 1998.

<sup>35</sup> See, e.g., Walsh, December, 1997; Letter to the Select Committee from Sandra Taylor, Vice-President, Eastman Kodak Company, November 18, 1998.

<sup>36</sup> Walsh, December 1997. See also Joseph Kahn, “McDonnell’s Hopes in China Never Got Off the Ground,” *The Wall Street Journal*, May 22, 1996 (quoting McDonnell’s President as saying it should do “whatever it takes” to “carve out a place” in China).

<sup>37</sup> Walsh Testimony and Letter to the Select Committee from Sandra Taylor, Vice-President, Eastman Kodak Company, November 18, 1998.

<sup>38</sup> Letter to the Select Committee from Sandra Taylor, Vice-President, Eastman Kodak Company, November 18, 1998.

<sup>39</sup> See John Frankenstein, “China’s Defense Industries: A New Course?” The Chinese concept of a “spin-on” is in marked contrast to the “spin-off” approach of the US at the end of the Cold War, where the goal was to convert military technology to commercial uses.

<sup>40</sup> “News Digest,” *Helicopter News*, March 28, 1997. “The Z-11 is a reverse-engineered copy of Eurocopter’s single-engined Ecureuil.”

<sup>41</sup> This Ministry is now known as the Ministry of Information Industry.

<sup>42</sup> “Sale of Telecommunications Equipment to China,” Karen Zuckerstein, David Trimble, and John Neumann, General Accounting Office, November 1996.

<sup>43</sup> Testimony of James Mulvenon, October 15, 1998.

<sup>44</sup> Interview of Tom Nangle, October 8, 1998.

<sup>45</sup> Almost all Chinese military production lines are co-located with civil/commercial production lines.

<sup>46</sup> “Commercial Activities of China’s People’s Liberation Army (PLA),” Hearing Before the Committee on Foreign Relations, United States Senate, November 6, 1997.

<sup>47</sup> Testimony of James Mulvenon, October 15, 1998.

<sup>48</sup> *Ibid.*

<sup>49</sup> Interview of Bin Wu, October 20, 1998. See also John Fialka, “War by Other Means,” W.W. Norton and Co., New York (1997).

<sup>50</sup> *Ibid.*

<sup>51</sup> *Ibid.*

<sup>52</sup> “Aegis Combat System,” United States Navy Fact File.

<sup>53</sup> Letter from FBI Director Louis Freeh to Chairman Christopher Cox and Ranking Member Norman Dicks, November 10, 1998. Peter Lee refused to cooperate with the Cox Committee’s investigation on the advice of his lawyer not to testify before, or provide information to, the Cox Committee.

<sup>54</sup> Ronald Ostrow, “FBI Arrests Chinese National in Spy Ring Investigation,” *Los Angeles Times*, December 5, 1993; Bill Gertz, “Spy Sting Gets Chinese Man Deported,” *The Washington Times*, December 22, 1993.

---

<sup>55</sup> Ibid.

<sup>56</sup> "DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories," Gary L. Jones et. al., General Accounting Office, September 1997.

<sup>57</sup> Ibid.

<sup>58</sup> "Chinese Spies Just as Active as Soviets Ever Were, FBI Says," Ruth Sinai, Associated Press, March 9, 1992. Statements in article are attributed to Patrick Watson, the FBI's Deputy Assistant Director for Intelligence.

<sup>59</sup> Testimony of Nicholas Eftimiades, October 15, 1998.

<sup>60</sup> "Chinese Intelligence Operations," Nicholas Eftimiades, Naval Institute Press, 1994.

<sup>61</sup> Ibid.

<sup>62</sup> "Chinese spy openly at weapons fair," Kenneth R. Timmerman, *The Washington Times*, March 24, 1997.

<sup>63</sup> "Department of Defense Disposition of Government Surplus Items," hearing before the Senate Judiciary Subcommittee on Administrative Oversight and the Courts, July 8, 1997; "Defense Inventory: Action Needed to Avoid Inappropriate Sales of Surplus Parts," General Accounting Office, August, 1998; "On the Introduction of The Arms Surplus Reform Act of 1997," statement by Rep. Pete Stark in the US House of Representatives, October 1, 1997.

<sup>64</sup> Ibid.

<sup>65</sup> Ibid.

<sup>66</sup> US Customs briefing to Select Committee Staff, October 28, 1998. In response to this situation, in October 1997, Representative Pete Stark introduced H.R. 2602, the Arms Surplus Reform Act of 1997, to place a moratorium on all surplus arms sales until DOD certified to Congress that steps had been taken to correct weaknesses in the surplus sales program. The Act did not pass, but a section was added to the Defense authorization Act for Fiscal Year 1998, Pub. L. 105-85, Sec. 1067, requiring similar steps. The DOD submitted its report to Congress in June, 1998, identifying problem areas and steps taken to address them.

<sup>67</sup> Robert Greenberger, "Let's Make a Deal: Chinese Find Bargains in Defense Equipment as Firms Unload Assets," *Wall Street Journal*, October 21, 1998; Dr. Stephen Bryen and Michael Ledeen, "China-Related Challenges," *Heterodoxy*, April/May 1997 (Submission for the record by Rep. Tillie Fowler in the US House of Representatives, June 26, 1997).

<sup>68</sup> Robert Levy, President, Norman Levy Associates, as quoted in Robert Greenberger, "Let's Make a Deal: Chinese Find Bargains in Defense Equipment as Firms Unload Assets," *Wall Street Journal*, October 21, 1998.

<sup>69</sup> Interview of Jerry Remick, October 8, 1998; Interview of David Duquette, October 14, 1998. In a response to

written interrogatories, officials of CATIC, USA denied it was aware of the existence of the US company. Letter to Daniel Silver from Barbara Van Gelder, October 22, 1998.

<sup>70</sup> "Message to the Congress on the China National Aero-Technology Import and Export Corporation Divestiture of MAMCO Manufacturing, Incorporated," The White House, February 1, 1990.

<sup>71</sup> Bruce Einhorn, "The China Connection," *Business Week*, August 5, 1996: "Sunbase Asia Acquires Specialty Bearing Company," PR Newswire, January 17, 1996.

<sup>72</sup> Briefing by US Treasury Department to Select Committee staff, October 29, 1998.

<sup>73</sup> See, e.g., Stan Crock, "China and the US: The Sparks May Start Flying," *Business Week*, November 16, 1998; Robert Little, "Controversial Carrier," *The Baltimore Sun*, November 8, 1998.

<sup>74</sup> See, e.g., Timothy Maier, "Long March Reaches Long Beach," *Insight*, September 8, 1997.

<sup>75</sup> Interview of Wu Bin, October 20, 1998.

<sup>76</sup> Bruce Smith, "Dragonair Misstep," *Aviation Week and Space Technology*, September 16, 1996; "Michael Mecham, "China Expands Stake in Cathay, Dragonair," *Aviation Week and Space Technology*, May 6, 1996.

<sup>77</sup> See, e.g., "Hong Kong's Reversion to China: Effective Monitoring Critical to Assess US Nonproliferation Risks," GAO, May, 1997.

<sup>78</sup> US Customs briefing to Select Committee Staff, October 28, 1998.

<sup>79</sup> Kathleen A. Walsh, "US Technology Transfers to the People's Republic of China," 1997.

<sup>80</sup> Testimony of Loren Thompson, Clayton Mowry and Ray Williamson, November 13, 1998; deposition of C. Michael Armstrong, November 17, 1998.

<sup>81</sup> Deposition of Bernard L. Schwartz, November 21, 1998; testimony of Clayton Mowry, November 13, 1998.

<sup>82</sup> Deposition of Bernard L. Schwartz, November 21, 1998.

<sup>83</sup> Deposition of C. Michael Armstrong, December 17, 1998.

<sup>84</sup> Ibid.

<sup>85</sup> Deposition of C. Michael Armstrong, December 17, 1998; letter from C. Michael Armstrong, Bernard L. Schwartz, and Daniel Tellep to the President, October 6, 1995.

<sup>86</sup> Aerospace Industries Association, "Presidential Satellite Waivers and Other Related Launch Information" ([http://www.aia-aerospace.org/homepage/china\\_table1](http://www.aia-aerospace.org/homepage/china_table1)), October 26, 1998.

---

<sup>87</sup> Far Eastern Economic Review, January 23, 1997.

<sup>88</sup> Deposition of Bansang Lee, November 16, 1998. CP divested itself of its holdings in APT in late 1997. See Jonathan Sprague and Julian Gearing Bangkok, "Past Ambitions Catch Up To Charoen Pokphand," Asiaweek, May 15, 1998.

<sup>89</sup> SCGA Report.

<sup>90</sup> Testimony of Karl Jackson before the SCGA, September 16, 1997; testimony of Clark Southall Wallace before the SCGA, September 16, 1997; testimony of Beth Dozoretz before the SCGA, September 16, 1997.

<sup>91</sup> Premier Zhu Rongji recently praised the efforts and progress of PRC and US scientists who attended the 19th Meeting of the Sino-US Joint Committee on High Energy Physics. Reportedly, Zhu expressed pleasure that the "two nations have conducted wide-ranging in-depth exchanges during the meeting and put forward many helpful proposals, which will not only be conducive to the development of high energy physics in PRC and the US, but also help expand scientific and technological cooperation between the two countries." An area of concern is the PRC intelligence practice of mining even ostensibly cooperative scientific exchanges for useful information. "Premier Meets US Science Group," China Daily, November 18, 1998.

<sup>92</sup> See Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories, Government Accounting Office, October 1988; DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories, Government Accounting Office, September 1997; and, DOE Needs to Improve Controls Over Foreign Visitors To Its Weapons Laboratories, Government Accounting Office, October 14, 1998.

<sup>93</sup> A "walk-in" is an individual who voluntarily offers to conduct espionage. The Encyclopedia of Espionage defines a "walk-in" as "an unheralded defector or a dangle, a 'walk-in' is a potential agent or a mole who literally walks into an embassy or intelligence agency without prior contact or recruitment." See the Spy Book: The Encyclopedia of Espionage, by Norman Polmar and Thomas B. Allen (RH Reference & Information Publishing, Random House). The individual who approached the CIA in 1995 is suspected of being a "directed walk-in": a "walk-in" purposefully directed by the PRC to provide this information to the United States. There is speculation as to the PRC's motives for advertising to the United States the state of its nuclear weapons development.

<sup>94</sup> Department of Defense, The Militarily Critical Technologies List. Part I: Weapons Systems

Technologies (Washington, D.C.: US Department of Defense, June 1996).

<sup>95</sup> The machine tool diversion reportedly remains under investigation by the Department of Justice.

<sup>96</sup> DIA report, 1995. See also The Militarily Critical Technologies List. Part I: Weapons Systems Technologies, Department of Defense, June 1996, sec. 10; and "Report of Foreign Travel," Ronald V. Miskell, US Department of Energy, February 1998.

<sup>97</sup> China Today: Defense Science and Technology, Xie Guang, ed., Beijing National Defense Industry Press, 1993; and Gearing up for High-Tech Warfare, Richard Bitzinger and Bates Gill, Center for Strategic and Budgetary Assessments, 1996. <sup>80</sup> See also The Militarily Critical Technologies List. Part I: Weapons Systems Technologies, Department of Defense, June 1996, sec. 1.

<sup>98</sup> "PLAAF & Aviation Production Overview," Kenneth W. Allen, Henry L. Stimson Center, Washington, D.C., 1998.

<sup>99</sup> Background Paper, Defense Intelligence Agency, 1993.

<sup>100</sup> Ibid.

<sup>101</sup> Memorandum for the Record, December 17, 1998. William Schneider described this incident during a briefing on the dual-use applications of high performance computers. William Schneider, briefing on "High Performance (HPC) Exports to China," October 1, 1998. See also Defense Intelligence Agency, 1993.

<sup>102</sup> Defense Intelligence Agency, 1993.

<sup>103</sup> Background Paper, Defense Intelligence Agency, 1993.

<sup>104</sup> Export Controls: Change in Export Licensing Jurisdiction for Two Sensitive Dual-Use Items GAO/NSIAD-97-24, January 1997, p. 5, (B22); and The Militarily Critical Technologies List. Part I: Weapons Systems Technologies, Department of Defense, June 1996, sec. 1.

<sup>105</sup> Memorandum for the Record, October 30, 1998.

<sup>106</sup> "PLAAF & Aviation Production Overview," Kenneth W. Allen, Henry L. Stimson Center, Washington, D.C., 1998.

<sup>107</sup> China's Aerospace Industry, Jane's Information Group, 1997, pp. 67, 70, (B172); and "PRC Gas Turbine Acquisition Efforts" Memorandum by Peter Leitner, Defense Technology Security Administration, September 1, 1992.

<sup>108</sup> China's Aerospace Industry, Jane's Information Group, 1997.

<sup>109</sup> Ibid.

<sup>110</sup> "PRC Gas Turbine Acquisition Efforts" Memorandum by Peter Leitner, Defense Technology Security

---

Administration, September 1, 1992; and “Garrett Engine Case,” Memorandum from Peter Leitner, DTSA, to Barbara Dixon, Defense Intelligence Agency, July 21, 1992.

<sup>111</sup> China’s Aerospace Industry, Jane’s Information Group, 1997.

<sup>112</sup> “WP-11 Engine Information,” James Clauson, Jane’s Information Group, June 26, 1996.

<sup>113</sup> Ibid.

<sup>114</sup> Memorandum for the Assistant Secretary of Defense for International Security Affairs, January 7, 1993.

<sup>115</sup> “Cruise Control: Relaxed US Export Controls Could Help China Build Stealthier and Longer-Range Cruise Missiles, Pentagon Officials Claim,” Nigel Holloway, *Far Eastern Economic Review*, August 14, 1997; and “Williams FJ44,” Jane’s All the World’s Aircraft 1990-1991, Jane’s Information Group, 1990.

<sup>116</sup> “Morphing the Silkworm,” Dennis Gormley and Gregory DeSantis, Pacific-Sierra Research Corporation, Arlington, Virginia, Presentation to the Rumsfeld Commission, June 3, 1998; and China’s Aerospace Industry, Jane’s Information Group, 1997.

<sup>117</sup> “Cruise Control: Relaxed US Export Controls Could Help China Build Stealthier and Longer-Range Cruise Missiles, Pentagon Officials Claim,” Nigel Holloway, *Far Eastern Economic Review*, August 14, 1997.

<sup>118</sup> “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>119</sup> Memorandum for the Record, Review of State Department Cables Regarding Allied Signal/Garrett Jet engine Negotiations with the PRC, December 17, 1998. The relevant State Department cable- DTG 161312Z July 92, #0148838-0148839-was sent to Commerce, State and Defense. See also “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>120</sup> A history of the Garrett case is presented in “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of

Defense (Trade Security Policy) and DTSA Director, December 21, 1992. See also “Issue Paper on Garrett Engine Sale to PRC,” Attachment to “Export of Garrett Engines to the PRC,” Memorandum from Peter M. Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992.

<sup>121</sup> “NAMC/PAC K-8 Karakorum,” Richard L. Aboulafia, World Military & Civil Aircraft Briefing, Teal Group Corp., Arlington, Virginia, March 1998.

<sup>122</sup> “NAMC/PAC K-8 Karakorum,” Richard L. Aboulafia, World Military & Civil Aircraft Briefing, Teal Group Corp., Arlington, Virginia, March 1998.

<sup>123</sup> Memorandum from Peter Leitner to Peter Sullivan, Defense Technology Security Administration, December 30, 1992.

<sup>124</sup> “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>125</sup> “Type Certification Data Sheet No. E6WE,” Federal Aviation Administration, March 23, 1998.

<sup>126</sup> The Federal Aviation Administration can certify a jet engine as “civil” if it meets certain safety and other requirements for civil aviation. Military engines that meet such requirements can be certified as civil through this process. A civil certification places the engines on the Commerce Control List, giving Commerce authority to license exports, pursuant to Export Administration Act Section 17(c) on Civil Aircraft Equipment. However, Section 17(c) states that Commerce has jurisdiction over civil aircraft equipment that “is to be exported to a country other than a controlled country.” The PRC was a “controlled country” during the time of the Garrett case. Iain Baird believed that in-as-much as the statute mandated inclusion of civil aircraft engines to some destinations on the Commerce Control List (CCL), it was decided to put the item as a whole on the list. Commerce was unable to provide a formal legal analysis of 17 (c) with respect to exports of civil aircraft equipment to controlled countries. Civil certification issues and EAA Section 17(c) are discussed in, Interview of Iain S. Baird, November 17, 1998; and Interview of Bruce C. Webb, December 2, 1998. For the response to the Select Committee’s request for records regarding commodity jurisdiction, see letter from John F.



---

Sopko, Chief Counsel for Special Matters, Department of Commerce, to Chairman Christopher Cox and Ranking Member Norm Dicks, December 14, 1998.

<sup>127</sup> “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>128</sup> Ibid.

<sup>129</sup> Ibid.

<sup>130</sup> Ibid.

<sup>131</sup> Ibid.

<sup>132</sup> Ibid.

<sup>133</sup> Ibid.

<sup>134</sup> “Type Certification Data Sheet No. E6WE,” Federal Aviation Administration, March 23, 1988.

<sup>135</sup> “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>136</sup> Ibid.

<sup>137</sup> The revised Export Administration Regulations are presented in Export Administration Regulations, Department of Commerce, Bureau of Export Administration, 1991, sections 9A01 and 9E03. FADECs are described in Interview of Bruce C. Webb, December 2, 1998; and The Militarily Critical Technologies List. Part I: Weapons Systems Technologies, Department of Defense, June 1996, sec.1.

<sup>138</sup> Interview of Bruce C. Webb, December 2, 1998.

<sup>139</sup> “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>140</sup> Ibid.

<sup>141</sup> Ibid.

<sup>142</sup> Ibid.

<sup>143</sup> Commerce Form Letter to Allied Signal from Commerce Licensing Officer E.G. Christiansen, Subject: Advice on Amendment Request Returned Without Action, November 25, 1991; “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVLD130990,” Memorandum

from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>144</sup> “Issue Paper on Garrett Engine Sale to PRC,” Attachment to “Export of Garrett Engines to the PRC,” Memorandum from Peter M. Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992.

<sup>145</sup> “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>146</sup> Interview of Bruce C. Webb, December 2, 1998.

<sup>147</sup> For the request for records, see letter from Chairman Christopher Cox and Ranking Member Norm Dicks to William M. Daley, Secretary of Commerce, November 20, 1998. For Commerce’s response, see letter from John F. Sopko, Chief Counsel for Special Matters, Department of Commerce, to Chairman Christopher Cox and Ranking Member Norm Dicks, December 14, 1998.

<sup>148</sup> For the request for records, see letter from Chairman Christopher Cox and Ranking Member Norm Dicks to William M. Daley, Secretary of Commerce, November 20, 1998. <sup>139</sup> Interview of Peter Leitner, November 24, 1998.

<sup>149</sup> “Issue Paper on Garrett Engine Sale to PRC,” Attachment to “Export of Garrett Engines to the PRC,” Memorandum from Peter M. Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992.

<sup>150</sup> “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>151</sup> “Issue Paper on Garrett Engine Sale to PRC,” Attachment to “Export of Garrett Engines to the PRC” Memorandum from Peter M. Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992; and “Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990,” Memorandum



---

from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>152</sup> "Report to the Congress: Imposition of Foreign Policy Export Controls Under the Enhanced Proliferation Control Initiative," Department of Commerce, Bureau of Export Administration, February 1991.

<sup>153</sup> "Imposition and Expansion of Foreign Policy Controls," Department of Commerce, Bureau of Export Administration, August 15, 1991.

<sup>154</sup> Interview of Iain S. Baird, November 17, 1998.

<sup>155</sup> See letter from John F. Sopko, Chief Counsel for Special Matters, Department of Commerce, to Chairman Christopher Cox and Ranking Member Norm Dicks, December 14, 1998.

<sup>156</sup> Memorandum from Defense Intelligence Agency, 1992.

<sup>157</sup> "WP-11 Engine Information," James Clauson, Jane's Information Group, Alexandria, Virginia, June 26, 1996.

<sup>158</sup> Memorandum to Ken Weiss, Arms Control; and Disarmament Agency, 1993; and Defense Intelligence Agency.

<sup>159</sup> F. Michael Maloof, Director, Technology Security Operations, DTSA, to US Department of Commerce, August 11, 1992.

<sup>160</sup> Interview of Peter Leitner, November 24, 1998. See also letter from F. Michael Maloof, Director, Technology Security Operations, DTSA, to US Department of Commerce, August 11, 1992.

<sup>161</sup> "Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990," Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>162</sup> See "Issue Paper on Garrett Engine Sale to PRC," Attachment to "Export of Garrett Engines to the PRC," Memorandum from Peter Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992. See also "Garrett TFE-731-2A," Memorandum from M. Agnello, Senior Engineer, Controls & Integrated Systems, Naval Air Warfare Center, to Charles H. Craig, Senior Engineer, Technical Directorate, DTSA/OSD, November 30, 1993; and "Engineering Analysis and Technical Policy Recommendations of General Exception Status in CoCom of DOC IVL D130990," Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy

Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>163</sup> "Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990," Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>164</sup> Ibid.

<sup>165</sup> Ibid.

<sup>166</sup> "China Shops: Fact from Fiction," Fact sheet attached to "The China Shop Fact Sheet," Memorandum to Mark Kron from Iain S. Baird, Deputy Assistant Secretary for Export Administration, Department of Commerce, February 26, 1995.

<sup>167</sup> "Gas Turbine Engines," Aviation Week & Space Technology, January 12, 1998; and "AlliedSignal TFE731," Jane's All the World's Aircraft 1995-96, Jane's Information Group, 1995.

<sup>168</sup> "Engineering Analysis and Technical Policy Recommendation of General Exception Status in CoCom of DOC IVL D130990," Memorandum from Clarence M. Griffin, Director, DTSA Technology Directorate, to the Acting Deputy Undersecretary of Defense (Trade Security Policy) and DTSA Director, December 21, 1992.

<sup>169</sup> Letter from Martha Harris, Deputy Assistant Secretary for Export Controls, Bureau of Political Military Affairs, Department of State, to Mitchel B. Wallerstein, Deputy Assistant Secretary of Defense, Counterproliferation Policy, April 1, 1994.

<sup>170</sup> Interview of Peter Leitner, November 24, 1998.

<sup>171</sup> Interview of Iain S. Baird, November 17, 1998.

<sup>172</sup> Interview of Bruce C. Webb, December 2, 1998.

<sup>173</sup> For the request for records, see letter from Chairman Christopher Cox and Ranking Member Norm Dicks to William M. Daley, Secretary of Commerce, November 20, 1998. For Commerce's response, see letter from John F. Sopko, Chief Counsel for Special Matters, Department of Commerce, to Chairman Christopher Cox and Ranking Member Norm Dicks, December 14, 1998.

<sup>174</sup> "Export of Garrett Engines to the PRC," Memorandum from Peter M. Sullivan, Acting Deputy Under Secretary of Defense for Technology Security Policy, to Deputy Secretary of Defense, December 29, 1992.

<sup>175</sup> Letter from Mitchel B. Wallerstein, Deputy Assistant Secretary of Defense, Counterproliferation Policy, to Martha Harris, Deputy Assistant Secretary for Export Controls, Bureau of Political Military Affairs, Department of State, March 21, 1994.

<sup>176</sup> Interview of Mitchel B. Wallerstein, November 25, 1998.

<sup>177</sup> Letter from Martha Harris, Deputy Assistant Secretary for Export Controls, Bureau of Political Military Affairs, Department of State, to Mitchel B. Wallerstein, Deputy Assistant Secretary of Defense, Counterproliferation Policy, April 1, 1994.

<sup>178</sup> "OCM 93-271/D184525-Allied Signal Aerospace Co.-Eighteen Garrett Engines," Meeting record for the Operating Committee on Export Policy, August 19, 1993.

<sup>179</sup> "Allied Signal Ends Plans to Coproduce Engines in China," Eduardo Lachica, *The Wall Street Journal*, October 27, 1995.

<sup>180</sup> Ibid.

<sup>181</sup> "China Aviation Project in Doubt," South China Morning Post, May 15, 1996.

<sup>182</sup> US Technology Transfers to the People's Republic of China, Kathleen Walsh, DFI International, Washington, D.C., December 1997.

<sup>183</sup> China's Aerospace Industry, Jane's Information Group, 1997.

<sup>184</sup> United Technologies Corporation's Responses to Written Interrogatories, November 16, 1998.

<sup>185</sup> Ibid.

## **White House Response to Cox Report** **1 February 1999**

In his response to the Cox Report, President Clinton agreed with the need to maintain effective measures to prevent the diversion of US technology and to prevent unauthorized disclosure of sensitive military information. We also agree with the Committee's recommendation to support US high-tech competitiveness consistent with national security. This has been a longstanding premise of the Clinton Administration's technology transfer policies.

In this regard, the Administration agrees with the substance of nearly all the Committee's recommendations, many of which we have been implementing for months, and in some cases, years. We have worked cooperatively with the Committee to declassify as much of the report as possible so that the American public can be informed on these important issues, consistent with the need to protect sensitive national security and law enforcement information. The declassified report, released today, provides the Committee's detailed assessments and investigations underlying its recommendations. Although the Administration does not agree with all of the Committee's analysis, we share the Committee's objective of strengthening export controls and counterintelligence, while encouraging legitimate commerce for peaceful purposes. With regard to the specific issues raised in the report:

### **Security at US National Laboratories**

The Administration is deeply concerned about the threat that China and other countries are seeking to acquire sensitive nuclear information from the US National Laboratories. Security at the labs has been a long-term concern, stretching back more than two decades. In 1997, the Administration recognized the need to respond to this threat with a systematic effort to strengthen counterintelligence and security at the US National Laboratories. In response, President Clinton issued a Presidential Decision Directive (PDD-61) in February 1998. This directive is the most comprehensive and

---

vigorous attempt ever taken to strengthen security and counterintelligence procedures at the labs. The FBI, in cooperation with DOE, is continuing its investigation into the possible source and extent of sensitive information that China may have acquired.

We welcome the Select Committee's support for PDD-61. As the President indicated in February, the Administration agrees with all of the Committee's recommendations concerning lab security, and we are carrying out these recommendations:

- The President asked the Director of Central Intelligence (DCI) to conduct a formal Intelligence Community damage assessment on China, which was reviewed by an independent panel headed by Admiral David Jeremiah. This review was completed and briefed to Congress on 21 April 1999.
- The DCI will, at the President's direction, also consider the recommendations made by Admiral Jeremiah's group on intelligence collection and resources.
- President Clinton asked the DOE to lead an interagency assessment of lab-to-lab programs with China, Russia, and other sensitive countries, which is scheduled for completion on 1 June 1999. The Administration believes that these programs serve the national security interest, but we are committed to ensuring that appropriate protections are in place to prevent compromise of classified information.
- Energy Secretary Bill Richardson is aggressively implementing PDD-61 on an expedited basis, and has been following the implementation plan that was submitted to Congress on 5 January 1999. By the end of 1999, the DOE CI program will be as good as the best in the US Government.
- Secretary Richardson has instituted a number of additional actions to improve counterintelligence security and safeguards at the National Laboratories, including in the critical area of cyber security. Secretary Richardson ordered a 14-day 'stand-down'

of all classified computers at the weapons labs, has initiated a massive reorganization of department security functions, and has greatly increased the cyber security posture at DOE.

- On 29 March 1999, the Department of Energy submitted to Congress its annual *Report Safeguards and Security at the Department of Energy Nuclear Weapons Facilities*. The report found that no nuclear material at DOE was at risk, but rated some areas 'marginal'. DOE initiated a thorough upgrade of all physical security and has committed to making all necessary upgrades so that all sites receive the highest rating by January 2000.
- The DCI, in coordination with appropriate agencies, is preparing a semi-annual report to Congress on the measures that are being taken to protect against espionage efforts by China to obtain nuclear weapons and other national security information of strategic concern.

In addition to the above steps recommended by the Select Committee, the President has requested Senator Warren Rudman, as Chairman of the bipartisan President's Foreign Intelligence Advisory Board, to evaluate security at the labs. Senator Rudman has assembled an excellent team of Board members to examine the issue. Finally, the President asked the National Counterintelligence Policy Board to recommend measures to strengthen controls over nuclear information at facilities aside from the National Laboratories that handle nuclear weapons issues.

## **Missile and Space Technology**

The Administration agrees with the Select Committee on the need to ensure that the launch of US-manufactured civilian satellites by China or any other foreign country does not inadvertently transfer missile technology. The Department of Justice is continuing to investigate the allegations of improper transfers cited by the report, and it is inappropriate to comment on the specifics of these cases. The Administration also agrees with the

---

Committee on the need to establish procedures to ensure timely processing of licenses, consistent with national security.

In this regard, the Administration agrees with and is carrying out all of the Committee's recommendations concerning satellite launches:

- The Administration has implemented the provisions of the FY 1999 Defense Authorization Act by, among other things, transferring licensing for communications satellite exports from the Department of Commerce to the Department of State.
- The Department of State has developed new procedures for timely review of licenses and is increasing its licensing staff to ensure the procedures are implemented properly.

The Department of State has taken steps to ensure that the affected US companies understand and comply with the requirements of law and regulation for data that may be provided to the space insurance industry. The Department of Defense (DoD) is implementing several measures proposed by the Committee to strengthen monitoring of foreign launches. Specifically:

- DoD has established a new organization called the Space Launch Monitoring Division within the Technology Security Directorate of the Defense Threat Reduction Agency and is hiring 39 additional staff for this function. The new division fulfills the Congressional requirement in the FY 1999 National Defense Authorization Act to recruit, train, and maintain a staff dedicated to all aspects of monitoring the export of space launch and satellite technology from the United States.
- The new dedicated, professional staff in DoD will provide end-to-end monitoring of controlled space launch and satellite technologies from the first export license application through to launch and failure analyses, if necessary. The monitors will review and approve all technology-transfer control plans, and all controlled technical data

proposed for export. Monitors will participate in all technical interchange meetings and other discussions involving controlled technical data. Monitors will also deploy to launch sites as a cohesive group with expertise in space launch security operations and satellite and launch vehicle technologies.

- DoD to augment the full-time monitoring staff should that be necessary to meet temporary surges in requirements for monitoring of meetings and other activities. As well, State and DoD are requiring industry to establish electronic archiving of technical data to ensure a complete and readily accessible database of all controlled data exported as part of a satellite launch campaign.
- Training for the monitor staff is being enhanced through a program of initial and recurring training and evaluation. The training will be managed as a formal program through the Defense Threat Reduction Agency's training facilities at Kirkland Air Force Base in New Mexico. The program will encompass the complete monitoring activities outlined in the FY 1999 National Defense Authorization Act.
- Finally, DoD is examining the recommendation regarding contracting for security personnel to provide physical security at foreign launchsites. DoD looks forward to a dialogue with the appropriate congressional oversight committees on this matter.

The Administration is encouraging development of the US domestic launch industry to reduce our dependence on foreign launch services. Since 1994, the Administration has fostered the international competitiveness of the US commercial space launch industry by pursuing policies and programs aimed at developing new, lower cost US capabilities to meet both government and commercial needs. For instance, DoD is investing \$3 billion in partnership with US commercial space companies to develop and begin flying two competing families of Evolved Expendable Launch Vehicles (EELV) with a goal of

---

significantly reducing launch costs for government and commercial payloads.

For the longer term, NASA has committed nearly \$1 billion toward work with industry in developing and demonstrating technology for next-generation reusable launch vehicles (RLVs). NASA's goal is to reduce launch costs by a factor of 10 within 10 years. To address the shifting balance from mostly government to predominantly commercial space launches in the US, the Administration recently initiated an interagency review to assess the appropriate division of roles and responsibilities between government agencies and the US commercial space sector in managing the operation, maintenance, improvement, and modernization of the US space launch bases and ranges. Together, these measures comprise an effective strategy aimed at strengthening domestic US space launch capabilities and our industry's international competitiveness.

### **Domestic and International Export Policies**

The Administration agrees with the Committee that the end of the Cold War and dissolution of COCOM in 1994 has complicated efforts to control transfers of militarily important dual-use goods and technology. In this regard, the Administration agrees with the Committee on the desirability of strengthening the Wassenaar Arrangement to improve international coordination and reporting on the export of militarily useful goods and technology and to prevent transfers of arms and sensitive dual-use items for military end-uses if the situation in a region or the behavior of a state is or becomes a cause of serious concern to the participating states. All Wassenaar members currently maintain national policies to prevent such transfers to Iran, Iraq, Libya, and North Korea. We are making a concerted effort in 2001 to strengthen and enhance existing transparency mechanisms and to expand restraint measures. We do not believe that other countries are prepared to accept a legally binding international regime like COCOM directed against China and we are not seeking such

a regime. We note that a COCOM-style veto could act against US interests by letting other countries block US sales to our security partners.

The Administration agrees with the Committee on the need to enact a new Export Administration Act with new penalties. We have operated for too long without updated legislation in this very important area. The Administration will work with the appropriate committees in Congress and US industry to obtain a new Export Administration Act. The Administration believes that the existing dual-use export licensing system allows adequate time for careful review of license applications and provides effective procedures to take account of national security considerations in licensing decisions.

### **High-Performance Computers**

The Administration agrees with the Committee that we should encourage the sale of computers to China for commercial, but not military, purposes. The Administration has not licensed high-performance computers (HPCs) to China for military purposes.

As recommended by the Committee, we are reviewing the potential national security uses of various configurations of computers, the extent to which such computers are controllable, and the various consequences to the US industrial base of imposing export controls on such computers. Our target date for completing this review is May 1999.

We also agree with the Committee that we need the capability to visit US HPCs licensed for export to China to observe how they are being used. During President Clinton's visit to China in June 1998, we secured a long sought Chinese agreement to arrangements to conduct on-site visits in China to help verify the civilian use of HPCs and other dual-use technology. We have been working to expand and strengthen this arrangement. We believe that it is not possible to obtain agreement by China or any other country to a no-notice verification regime for US goods.



## Chinese Technology Acquisition and Proliferation Activities

The Administration is well aware that China, like other countries, seeks to obtain sensitive US technology for military uses. We maintain strict policies prohibiting the export to China of munitions and dual-use items for military use. As recommended by the Select Committee, the FBI and CIA plan to complete their annual comprehensive threat assessment of PRC espionage by the end of May 1999, and the Inspector Generals of State, Defense, Commerce, Energy, Treasury, and CIA expect to complete their review of export controls by June 1999.

The Administration agrees with the Select Committee on the need to obtain more responsible export behavior by China. Through our policy of engagement, we believe that significant gains have been realized on this front. For example, at our initiative, China has committed not to provide assistance to unsafeguarded nuclear facilities in Pakistan or elsewhere—a commitment we believe is being observed by Beijing—terminated assistance to Iran on a project of nuclear proliferation concern and refrained from new civil and military nuclear cooperation with Iran, stopped exports of C-802 cruise missiles to Iran, and strengthened export controls over nuclear and chemical weapons related materials. China has also, with our urging, ratified the Nuclear Nonproliferation Treaty and the Chemical Weapons Convention and has signed the Comprehensive Test Ban Treaty, which are the key pillars of the international nonproliferation regime. On regional security, China has provided concrete assistance in dealing with proliferation threats in North Korea and South Asia.

The Administration agrees with the Committee that we should seek Chinese adherence to the Missile Technology Control Regime (MTCR.) In June 1998, President Jiang announced that China would actively study MTCR membership. The Administration intends to continue actively pressing the Chinese on this issue and other proliferation issues of concern.

## China's High-Tech Espionage Textbook

Following is a review of an intelligence textbook in Chinese by Zhongwen, Huo, and Wang Zongxiao. *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence*. Beijing: Kexue Jishu Wenxuan Publishing Co., 1991; 361pages:

It is one thing to document on the basis of press reports, ministry decrees, and other news coming out of China about its backdoor efforts to obtain foreign defense technology. It is quite another thing to have detailed proof of these activities publicized by people who helped build China's worldwide intelligence network. Incredible as it seems, this frank account of China's longstanding program to siphon off Western military science and technology (S&T), written as a textbook for PRC intelligence officers, was sold openly in China for years.

You will not find the book in any bookstore or Chinese library today. After reporter Bruce Gilley broke the story of its publication in the 20 December 1999 issue of the *Far Eastern Economic Review* under the title "China's Spy Guide," a quiet struggle ensued between foreigners eager to procure original copies of the book and the PRC's literary custodians who wanted it out of circulation. Accordingly, some of the copies that made it out of China are missing important pages. Interested parties can find an intact book at the US Library of Congress (Q223 H86), where it had been gathering dust since August 1992.

What is unusual about this book, and the reason you cannot buy a complete copy today, is that it represents the first public acknowledgment by PRC officials of China's program to collect secret and proprietary information on foreign military hardware, especially that of the United States. The book is all the more intriguing in light of China's current media blitz to portray itself as a wellspring of indigenous R&D.

The book's authors reveal themselves as PRC intelligence officers with "more than thirty years

of experience in information collection.” Early drafts of chapters were written during their tenure as instructors at the Peoples Liberation Army’s National Defense S&T Information Center for use in training intelligence specialists. Its final version is a synthesis of practical tips on intelligence gathering with esoteric theory on the nature of information and collection, meant to serve as a reference guide for colleagues in “national defense information research.”

Although the authors complain that foreign technology collection is still in the germination stage,” it is evident from the detailed information they give that China’s intelligence apparatus was already world class a decade ago. Indeed, this is one of the few areas of “science” where China is truly competitive, as suggested by the following passage:

*China’s S&T intelligence cause has already been developing for more than 30 years. As of now, we have assembled a contingent of collection workers of considerable scale in approximately 4,000 intelligence organizations throughout all of China. We have also achieved preliminary results as far as establishing S&T intelligence sources.*

The authors describe an “all-China S&T intelligence system” that functions on multiple levels, including “comprehensive S&T intelligence centers” in provinces, cities, and autonomous regions. This system, they claim, was built out of recognition that traditional techniques used by scientists the world over to keep up with developments in their fields were insufficient to meet China’s special needs for economic and military construction. What China required was nothing less than a “transformation in collection work carried out with an eye to assembling the intellectual wealth of humanity.” Collection—as opposed to collaboration or creation—is seen by the authors as a necessary and cost-effective way to acquire competitive technologies.

China’s decision to invest heavily in “collection science” has borne fruit. As the authors note:

*While China’s information collection work has experienced many ups and downs during these 30-odd years, it has nevertheless made outstanding contributions to the rejuvenation of the S&T intelligence cause, the invigoration of science and technology, the construction of the national economy and the build up of national defense.*

The authors’ lament about “S&T collection” being in its infancy is hard to reconcile with the impact they claim pilfered technology has on national defense and with the sophistication of the intelligence organization they describe. This is evidenced in the detailed treatment they give to each stage of the intelligence process. One (80-page) chapter evaluates foreign technology sources, which turn out to be largely American.

*Information collection operators should regularly peruse reference books relevant to their affairs, such as the various subscription catalogues compiled by the China National Publications Import and Export Corporation, foreign book stores and Xinhua Book Store; and such reference materials as are often used by national defense S&T information collection operators, such as the U.S. Government Report Notifications and Index, Spaceflight S&T Report, and World Conferences.*

Another chapter covers in detail methods for storing and retrieving intelligence and for getting it to the right people in a timely fashion. An entire section of the book considers ways to determine consumer needs.

One of the book’s most striking aspects is the attention it gives to metrics to measure success, defined as the extent to which genuine intelligence needs are satisfied in time to make a difference. The authors address this issue comprehensively and with mathematical rigor. It is apparent that China is dead serious not only about collecting S&T intelligence but also about putting it to effective use.

---

## Operational Collection

The authors recognize that there are limits to any collection tasking and provide three possible collection strategies. The first and most extensive is for intelligence officers to compile all information produced by a targeted source. If this is not feasible, the next best method is to collect inclusive categories of information from the target. The last strategy is to collect specifically selected information. For example, “the collection may be directed to collect all of the London International Strategic Research Institute’s research reports; or it may be directed to get the complete sets of AD reported film information or all of the NASA film reportage.” The Institute of Electrical and Electronics Engineers (IEEE) information could be the directed target of collection; or the directed collection may be a book title or some concrete leads supplied by a consumer as a “means to get the goods.” The many foreign TV signals monitored by foreign installations, or signals of foreign broadcasting stations are also directed collection.

The operational collection is not done erratically. Chinese Government entities, according to the book, provide tasking against their needs or requirements. Even if these requirements are very specific, an environment “in which the targets are not absolutely definitive, and the information that is actually wanted lie within that framework” guides the actual collection. Collection, therefore, in the authors’ opinion, is not an easy task, and “there is an aspect of randomness about it that puts a high demand on the quality and expertise of the collection operator.” They further recognize that every scrap of collected information is not necessarily useful but when a valuable indication comes to light, it will have positive results.

The authors further add that to conduct selection activities without the guidance of collection policies and plans is like trying to “cook without rice.” It can’t be done blind, nor wrested out of thin air. It must be based on frequent investigation and study with the assistance of reference materials and reference manuals.

These reference materials are diverse in form and content, and they are scattered and not easily found, and they can be rather difficult to comprehend. Collection operators rely primarily on their daily searches, discoveries, and accumulations. Most of the reference materials used today include, advertisements in periodicals and databases, publication notifications, new book and new electronic publication announcements, databases, publisher’s price lists, academic conference forecasts, critical reviews in newspapers and magazines, and verbal accounts from experts and students.

To promote sales and expand distribution, domestic and foreign media sources periodically or randomly publish reference books that consumers use for reference in the process of making selections. They include subscription catalogues, publication catalogues, new book weeklies, and cumulative book lists. Although the primary purpose of reference book search and book list databases is for researchers to investigate and find materials, it is a convenient way for information collection operators to find leads to information sources.

More than 80 percent of all consumer requirements can be satisfied by overt information; therefore, if all of the information collected through whatever channels by all elements were put together to form a consultation network of shared information, under existing conditions researchers requirements could—for the most part—be satisfied.

## Open Sources

One of the most startling revelations in *Sources and Techniques* is the extent to which the Chinese military and defense industries rely on open-source information, particularly US and British, for weapons modernization. According to the spying manual, more than 80 percent of all Chinese spying focuses on open-source material obtained from government and private-sector information. The remaining 20 percent of the information is gathered through illicit means, including eliciting information from scientists at meetings, through

---

documents supplied by agents, or through electronic eavesdropping.

This fact contrasts with the Cox Report's emphasis on China's use of covert methods to obtain military secrets. It also adds a critical dimension to our understanding of Chinese collection techniques as focusing on cooperative agreements and the exploitation of overseas scientists.

Astronautics (AIAA) publications and Department of Energy reports, particularly nuclear power and weapons-related studies, "continue to get a great deal of attention from those engaged in national defense S&T work" and are regarded as an "intelligence source of great value." US military standards as revealed in public bid specifications, drawings, and handbooks receive detailed scrutiny.

The authors concede that collecting national defense S&T information is difficult because of security classifications, but not impossible. As they put it:

*There are no walls which completely block the wind, nor is absolute secrecy achievable. Invariably there will be numerous open situations in which things are revealed, either in a tangible or intangible form. By picking up here and there among the vast amount of public materials and accumulating information a drop at a time, often it is possible basically to reveal the outlines of some secret intelligence, and this is particularly true in the case of Western countries.*

As an example of the payoff for diligence, the authors cite a program to declassify documents on thermonuclear weapons at a US national laboratory in the 1970s that resulted in 19,400 documents being declassified in error. The book explains:

*This incident tells us that, on the one hand, absolute secrecy is not attainable, while on the other hand, there is a random element involved in the discovery of secret intelligence sources, and to turn this randomness into inevitability, it is*

*necessary that there be those who monitor some sectors and areas with regularity and vigilance.*

The authors state unequivocally that Western scientific journals "are the first choice of rank-and-file S&T personnel as well as intelligence researchers." They then provide the results of a "core periodical survey" run by China's National Defense S&T Intelligence Center, which lists the 56 most popular defense technology journals, including 33 from the United States and 12 more from the United Kingdom. Another list of 80 journals included 43 titles published in the United States, the most popular ones dealing with aerospace.

## Conferences

*Information collection is conducted through personal contacts, as in attending academic exchange conferences, technical exchange conferences, planning, demonstration, and appraisal meetings and through discussions between individuals. This is the procedure commonly used for collecting verbal information, but it is not limited to verbal information. Participation in consultative activities is also a person to person exchange procedure for collecting information.*

The Chinese manual notes, "It is also necessary to stress that there is still 20 percent or less of our intelligence that must come through the collection of information using special means, such as reconnaissance satellites, electronic eavesdropping, and the activities of special agents (purchasing or stealing) . . ."

So why did China, a country not known for its willingness to share state secrets, allow such a book to be published? Mr. Gilley in his *Far Eastern Economic Review* article attributed the release of *Sources and Techniques* to an "oversight," adding that it could not be published in the atmosphere that prevails today. True enough. But to someone familiar with the psychology of Chinese technology transfer there is another explanation that is both

more facile and disconcerting. China's commitment to expropriating foreign technology is so much a part of its R&D culture that the book's authors simply took acceptance of this behavior for granted.

Support for this hypothesis is found in the regularity with which tech-transfer schemes are reported in China's "open" press, particularly as they involve the targeting by Beijing of ethnic Chinese scientists overseas. It is also evident in the authors' demand that collection of foreign S&T intelligence be treated as a "science" in its own right. It would seem that China's claim to innovation, as it were, is not entirely disingenuous, at least as it applies to intelligence collection.

### Old-Fashioned Espionage

Regarding espionage, the report states: "It is also necessary to stress that there is still 20 percent or less of our intelligence that must come through the collection of information using special means, such as reconnaissance satellites, electronic eavesdropping and the activities of special agents purchasing or stealing, etc."

The report further states that direct contact with scientists and other spying targets "is the procedure commonly used for collecting verbal information, but it is not limited to verbal communications. Participation in consultative activities is also a person-to-person exchange procedure for collecting information."

The information is gathered from people and institutions, including government agencies, research offices, corporate enterprises, colleges and universities, libraries, and information offices.

## Report on the Investigation of Espionage Allegations Against Dr. Wen Ho Lee

8 March 2000

### Summary

While the full impact of the errors and omissions by the Department of Energy (DOE) and the Department of Justice (DOJ)—including the Federal Bureau of Investigation (FBI)—in the investigation of Dr. Wen Ho Lee requires reading the full report, this summary covers some of the highlights.

The importance of Dr. Lee's case was articulated at his bail hearing on 13 December 1999 when Dr. Stephen Younger, Assistant Laboratory Director for Nuclear Weapons at Los Alamos, testified:

*These codes, and their associated databases, and the input file, combined with someone that knew how to use them, could, in my opinion, in the wrong hands, change the global strategic balance.<sup>1</sup> (Emphasis added)*

Younger further noted about the codes Dr. Lee mishandled:

*They enable the possessor to design the only objects that could result in the military defeat of America's conventional forces . . . They represent the gravest possible security risk to . . . the supreme national interest.<sup>2</sup> (Emphasis added) A "military defeat of America's conventional forces" and "the gravest possible security risk to . . . the supreme national interest" constitute threats of obvious enormous importance.*

It would be hard—realistically impossible—to pose more severe risks to US national security.

Although the FBI knew that Dr. Lee had access to highly classified information, had repeated contacts with the PRC scientists, and lied about his activities, the FBI investigation was inept. In December 1982, Dr. Lee called a former employee of Lawrence Livermore National Laboratory (LLNL).



---

Although the Subcommittee's inquiry into the handling of the Dr. Wen Ho Lee investigation is not completed, important conclusions have been reached that require Congressional consideration of remedial legislation at the earliest possible time.

The purpose of counterintelligence is to identify suspicious conduct and then pursue an investigation to prevent or minimize access by foreign agents to our secrets. The investigation of Dr. Lee since 1982 has been characterized by a series of errors and omissions by the Department of Energy and the Department of Justice, including the FBI, which have permitted Dr. Lee to threaten US supremacy by putting at risk information that could change the "global strategic balance." This interim report will describe and discuss some of those errors and omissions and suggest remedial legislation.

Dr. Wen Ho Lee was investigated on multiple occasions during a 17-year period, but none of these investigations—or the security measures in place at Los Alamos—came close to discovering and preventing Dr. Lee from putting the national security at risk by placing highly classified nuclear secrets on an unsecured system where they could easily be accessed by even unsophisticated hackers.<sup>3</sup> Given all the indicators that were present, it is difficult to comprehend how officials entrusted with the responsibility for protecting our national security could have failed to discover what was really happening with Dr. Lee.

## **The Investigation of 1982-84**

Dr. Wen Ho Lee was born in Nantou, Taiwan, in 1939. After graduating from Texas A&M University with a doctorate in 1969, he became a US citizen in 1974 and began working at Los Alamos National Laboratory in applied mathematics and fluid dynamics in 1978.<sup>4</sup> The FBI first became concerned about Dr. Lee as a result of contacts he made with a suspected PRC intelligence agent in the early 1980s. On 3 December 1982, Dr. Lee called a former employee of Lawrence Livermore National Laboratory

(LLNL) who was suspected of passing classified information to the Peoples Republic of China (PRC). This call was intercepted pursuant to a Foreign Intelligence Surveillance Act (FISA) court-authorized wiretap in another FBI espionage investigation. After introducing himself, Dr. Lee stated that he had heard about the Lawrence Livermore scientist's "matter" and that Lee thought he could find out who had "squealed" on the employee.<sup>5</sup> On the basis of the intercepted phone call, the FBI opened an espionage investigation on Dr. Lee.

For the next several months, the FBI investigated Dr. Lee with much of the work being done under the guise of the periodic reinvestigation required for individuals with security clearances. On 9 November 1983, the FBI interviewed Dr. Lee. Before being informed that the FBI had intercepted his call to the Lawrence Livermore employee, Lee stated that he had never attempted to contact the employee, did not know the employee, and had not initiated any telephone calls to him. These representations were patently false.<sup>6</sup> During the course of this interview, Dr. Lee offered to assist the FBI with its investigation of the other scientist.

On 20 December 1983, the FBI again interviewed Dr. Lee,<sup>7</sup> this time in California. During this interview, Lee explained that he had been in contact with Taiwanese nuclear researchers since 1977 or 1978, had done consulting work for them, and had sent some information that was not classified but that should have been cleared with DOE officials. He tried to explain that he had contacted the subject of the other investigation because he thought this other scientist was in trouble for doing the same thing that Lee had been doing for Taiwan.<sup>8</sup> After this interview, the FBI sent Dr. Lee to meet with the espionage suspect. On the record currently available, that meeting did not produce anything.

On 24 January 1984, Dr. Lee took an FBI polygraph examination, which included questions about passing classified information to any foreign government, Lee's contacts with the Taiwanese Embassy, and his contacts with the LLNL scientist. Although the FBI has subsequently contended

that Dr. Lee's answers on this polygraph were satisfactory,<sup>9</sup> there remained important reasons to continue the investigation. His suspicious conduct in contacting the Lawrence Livermore scientist and then lying about it, the nature of the documents that he was sending to the Taiwanese Embassy, and the status of the person to whom he was sending those documents were potential danger signals. Although not classified, the documents Dr. Lee was passing to Taiwan's Coordination Council of North America were subject to Nuclear Regulatory Commission export controls. They were specifically stamped "no foreign dissemination." According to the testimony of FBI Special Agent Robert Messemer at a special hearing on 29 December 1999, FBI files also contain evidence of other "misrepresentations" that Dr. Lee made to the FBI during the period 1983-84 that have raised "grave and serious concerns" about Dr. Lee's truthfulness. For security reasons, these matters cannot be further detailed.<sup>10</sup> Notwithstanding these reasons for continuing the investigation, the FBI closed its initial investigation of Lee on 12 March 1984.<sup>11</sup>

During the course of the 1982-84 investigation, it was clear that, by virtue of his work assignment and access to top nuclear secrets, Dr. Lee was in a position to do considerable damage to the national security. Thus, suspicions of espionage or a lack of trustworthiness should have been treated with great concern. On the state of the record, consideration should have been given to suspending his access to classified information, and, at a minimum, an intensified investigation should have been pursued. Instead, the FBI permitted him to stay in place, which enabled him to undertake a course of conduct—years later—leading to his potential to change the global strategic balance.

The 1982-84 investigation of Dr. Lee represents a missed opportunity to protect the nation's secrets. Had the matter been handled properly, Dr. Lee's clearance and access would most likely have been removed long ago before he was able to put the global strategic balance at risk.

## **The Investigation of Dr. Lee From 1994 to 2 November 1995**

This investigation of Dr. Lee was initiated based on the discovery that he was well acquainted with a high-ranking Chinese nuclear scientist who visited Los Alamos as part of a delegation in 1994.<sup>12</sup> Dr. Lee had never reported meeting this scientist, which he was required to do by DOE regulations, so his relationship with this person aroused the FBI's concern. Unclassified sources have reported that Dr. Lee was greeted by "a leading scientist in China's nuclear weapons program who then made it clear to others in the meeting that Lee had been helpful to China's nuclear program."<sup>13</sup> In concert with the 1982-84 investigation, Dr. Lee's undisclosed relationship with this top Chinese nuclear scientist should have alerted the FBI and the DOE that it was imperative to do an intensified investigation and reconsideration of his access to classified information. Instead, this FBI investigation was deferred on 2 November 1995 because Dr. Lee was by then emerging as a central figure in the Department of Energy's Administrative Inquiry (AI), which was developed by a DOE counterintelligence expert in concert with a seasoned FBI agent who had been assigned to DOE for the purposes of the inquiry. The DOE AI was given the code name Kindred Spirit.<sup>14</sup> The investigation of Dr. Lee was essentially dormant from November 1995 until May 1996, when the FBI received the results of the DOE AI and opened a new investigation of Dr. Lee on 30 May 1996.

It is difficult to understand why the FBI suspended the investigation in 1995, even to wait for the Kindred Spirit AI, when the issues that gave rise to the 1994-95 investigation remained valid and unrelated to the Kindred Spirit investigation. The key elements of the 1994-95 investigation are described in the Letterhead Memorandum (LHM) of 1997, which was prepared to support the request for a FISA search warrant. Specifically, the LHM describes the unreported contact with the top nuclear scientist,<sup>15</sup> and it makes reference to the "PRC using certain computational codes . . . which were later identified as something that [Lee] had unique access to."<sup>16</sup> Finally, the LHM states that,

---

“the Director subsequently learned that Lee Wen Ho had worked on legacy codes.”<sup>17</sup> Given these serious allegations, it was a serious error to allow the investigation to wait for several months while the DOE AI was being completed. This deferral needlessly delayed the investigation and left important issues unresolved.

In addition to information known to the FBI, which required further intensified investigation rather than the deferred investigation on 2 November 1995, the DOE was incredibly lax in failing to understand and pursue obvious evidence that Dr. Lee was downloading large quantities of classified information to an unclassified system. The sheer volume of Dr. Lee’s downloading showed up on a DOE report in 1993.<sup>18</sup> Cheryl Wampler, from the Los Alamos computer office of LLNL, has testified that the NADIR system—Network Anomaly Detection and Intrusion Recording—flagged Dr. Lee’s massive downloading in 1993.<sup>19</sup> This system is specifically designed to create profiles of scientists’ daily computer usage so it can detect unusual behaviors. A DOE official with direct knowledge of Lee’s suspicious activity failed to act on it or to tell DOE counterintelligence personnel or the FBI. On the basis of its design, the NADIR system would have continued to flag Dr. Lee’s computer activities in 1994 as being unusual, but no one from DOE took any action to investigate what was going on.<sup>20</sup> Also, Dr. Lee’s downloading of classified information was not mentioned to the FBI or DOE’s counterintelligence personnel.

Had DOE transmitted this information to the FBI, and had the FBI acted on it, Dr. Lee could have and should have been stopped in his tracks in 1994 on these indicators of downloading. The full extent of the importance of the information that Dr. Lee was putting at risk through his downloading was encapsulated in a document the government filed in December 1999 as part of the criminal action against Dr. Lee:

*[I]n 1993 and 1994, Lee knowingly assembled 19 collections of files, called tape archive (TAR) files, containing Secret and Confidential Restricted Data relating to atomic weapon*

*research, design, construction, and testing. Lee gathered and collected information from the secure, classified LANL computer system, moved it to an unsecured, “open” computer, and then later downloaded 17 of the 19 classified TAR files to nine portable computer tapes.*<sup>21</sup>

These files, which amounted to more than 806 megabytes, contained information that could do vast damage to the national security.

The end result of these missteps and lack of communication was that, during some of the very time that the FBI had an espionage investigation open on Dr. Lee resulting from his unreported contacts with a top Chinese scientist and the realization that the Chinese were using codes to which Dr. Lee had unique access, DOE computer personnel were being warned by the NADIR system that Dr. Lee was moving suspiciously large amounts of information around but were ignoring those warnings and were not passing them on to the FBI.

The near-perfect correlation between the allegations, which began the 1994-95 investigation and Dr. Lee’s computer activities, is stunning. The codes the Chinese were known to be using were computer codes, yet FBI and DOE counterintelligence officials never managed to discover these massive file transfers. Where, if not on his computer, were they looking? And, as for the lab computer personnel who saw but ignored the NADIR reports, what possible explanation can there be for a failure to conduct even the most minimal investigation?

### **The Investigation Renewed—30 May 1996 to 12 August 1997**

As noted previously, the investigation of Dr. Lee was dormant from 2 November 1995 until 30 May 1996.

In 1995, DOE scientists received information that raised the possibility that the Chinese had made significant technological advancements in warhead design. The now infamous “walk-in”

document was added to the equation in the summer of 1995. The walk-in document, coupled with concerns raised from a string of Chinese nuclear tests, led to the formal establishment of a DOE AI on 28 September 1995. As noted previously, at DOE's request, a senior FBI special agent was assigned to work this inquiry jointly with a DOE counterintelligence officer. This AI was presented to the FBI on 28 May 1996, and the FBI reopened its investigation of Dr. Lee on 30 May 1996.

The walk-in document is central to the Kindred Spirit investigation so it should be described in the greatest detail consistent with classification concerns. This document, dated 1988, is said to lay out China's nuclear modernization plan for Beijing's First Ministry of Machine Building, which is responsible for making missiles and nose cones.<sup>22</sup> The 74-page document contains dozens of facts about US warheads, mostly in a two-page chart. On one side of the chart are various US Air Force and US Navy warheads, including some older bombs as well as the W-80 warhead (cruise missiles), the W-87 (Minuteman III), and the W-88 (Trident II).<sup>23</sup> Among the most important items of information in the walk-in document are details about the W-88 warhead.

The *Cox Committee Report* provides the following description and assessment of the walk-in document:

*In 1995, a "walk-in" approached the Central Intelligence Agency outside of the PRC and provided an official PRC document classified "Secret" that contained design information on the W-88 Trident D-5 warhead, the most modern in the US arsenal, as well as technical information concerning other thermonuclear warheads.*

*The CIA later determined that the "walk-in" was directed by the PRC intelligence services. Nonetheless, the CIA and other Intelligence Community analysts that reviewed the document concluded that it contained US thermonuclear warhead design information.*

*The "walk-in" document recognized that the US nuclear warheads represented the state-of-the-art against which PRC thermonuclear warheads should be measured.*

*Over the following months, an assessment of the information in the document was conducted by a multidisciplinary group from the US government, including the Department of Energy and scientists from the US national weapons laboratories.<sup>24</sup>*

The Cox Committee's view that the Chinese had obtained sensitive design information about US thermonuclear warheads is bolstered by the June 1999 report of the President's Foreign Intelligence Advisory Board, which states that the walk-in document:

*Unquestionably contains some information that is still highly sensitive, including descriptions, in varying degrees of specificity, of the technical characteristics of seven US thermonuclear warheads.<sup>25</sup>*

When the FBI received notice that the source of the walk-in document was under the control of PRC intelligence services, however, the Kindred Spirit investigation was actually halted for a time, from 31 July 1996 until 20 August 1996. Even when it was restarted, it was not pursued with particular vigor in the latter part of 1996.

It is surprising that the investigation was halted, even for a few weeks, since it was conclusive that the walk-in document did contain important classified information, which had somehow fallen into the hands of a foreign power. The *Cox Committee Report* and the President's Foreign Intelligence Advisory Board have recently reconfirmed that the walk-in document was proof that the Chinese had obtained sensitive nuclear information, but there should never have been any doubt on the part of the FBI about that question in the summer of 1996. Moreover, the information, which led to the 1994-95 investigation, was no less valid because of any doubts about the walk-in document or even the Kindred Spirit Administrative Inquiry itself.



---

From 1996 until 1997 the DOE and FBI investigation was characterized by additional inexplicable lapses. For example, in November 1996, the FBI asked DOE counterintelligence team leader Terry Craig for access to Dr. Lee's computer. Although Mr. Craig apparently did not know it until 1999, Dr. Lee had signed a consent-to-monitor waiver<sup>26</sup> on 19 April 1995. The relevant portion of the waiver states:

*WARNING: To protect the LAN [local area network] systems from unauthorized use and to ensure that the systems are functioning properly, activities on these systems are monitored and recorded and subject to audit. Use of these systems is expressed consent to such monitoring and recording. Any unauthorized access or use of this LAN is prohibited and could be subject to criminal and civil penalties.*<sup>27</sup>

Moreover, the computer that Dr. Lee used apparently also had a banner, which had information that may have constituted sufficient notice to give the FBI access to its contents. And, finally, the Los Alamos National Laboratories (LANL) computer-use policy gave authorities the ability to search computers to prevent waste, fraud, and abuse.<sup>28</sup> As noted in the press release accompanying the Department of Energy Inspector General's Report of 12 August 1999, Mr. Craig's "failure to conduct a diligent search deprived the FBI of relevant and potentially vital information."<sup>29</sup> Had the FBI National Security Law Unit (NSLU) been given the opportunity to review these facts, it may well have concluded that no FISA warrant was necessary to conduct a preliminary investigation of Dr. Lee's computer. More important, records from the DOE monitoring systems like NADIR could almost certainly have been reviewed without a FISA warrant. Had these records been searched, Dr. Lee's unauthorized downloading would have been found nearly three years earlier. Unfortunately, through the failures of both DOE and FBI personnel, this critical information never reached FBI Headquarters, and the NSLU decided that Dr. Lee's computer could not be searched without a FISA warrant.<sup>30</sup> Thus, a

critical opportunity was lost to find and remove from an unsecured system information that could alter the global strategic balance.

Nonetheless, the FBI developed an adequate factual basis for the issuance of a FISA warrant. Senators Thompson and Lieberman of the Senate Committee on Governmental Affairs cogently summarized the information developed by the FBI to support its FISA application in 1997 in the special statement of 5 August 1999:<sup>31</sup>

1. DOE counterintelligence and weapons experts had concluded that there was a great probability that the W-88 information had been compromised between 1984 and 1988 at the nuclear weapons division of the Los Alamos laboratory.
2. It was standard PRC intelligence tradecraft to focus particularly upon targeting and recruitment of ethnic Chinese living in foreign countries (for example, Chinese-Americans).
3. It is common in PRC intelligence tradecraft to use academic delegations—rather than traditional intelligence officers—to collect information on science-related topics. It was, in fact, standard PRC intelligence tradecraft to use scientific delegations to identify and target scientists working at restricted US facilities such as LANL, since they "have better access than PRC intelligence personnel to scientists and other counterparts at the United States National Laboratories."
4. Sylvia Lee, wife of Wen Ho Lee, had extremely close contacts with visiting Chinese scientific delegations. Sylvia Lee, in fact, had volunteered to act as hostess for visiting Chinese scientific delegations at LANL when such visits first began in 1980 and had apparently had more extensive contacts and closer relationships with these delegations than anyone else at the laboratory. On one occasion, moreover, Wen Ho Lee had himself aggressively sought involvement with a visiting Chinese scientific



- 
- delegation, insisting upon acting as an interpreter for the group despite his inability to perform this function very effectively.
5. Sylvia Lee was involuntarily terminated at LANL during a reduction in force in 1995. Her personnel file indicated incidents of security violations and threats she allegedly made against coworkers.
  6. In 1986, Wen Ho Lee and his wife traveled to China on LANL business to deliver a paper on hydrodynamics<sup>32</sup> to a symposium in Beijing. He visited the Chinese laboratory—the Institute for Applied Physics and Computational Mathematics (IAPCM)—that designs the PRC’s nuclear weapons.
  7. The Lees visited the PRC—and IAPCM—on LANL business again in 1988.
  8. It was standard PRC intelligence tradecraft, when targeting ethnic Chinese living overseas, to encourage travel to the “homeland”—particularly where visits to ancestral villages and/or old family members could be arranged—as a way of trying to dilute loyalty to other countries and encouraging solidarity with the authorities in Beijing.
  9. The Lees took vacation time to travel elsewhere in China during their two trips to China in 1986 and 1988.
  10. The FBI also learned of the Lees’ purchase of unknown goods or services from a travel agent in Hong Kong while on a trip to that colony and to Taiwan in 1992. On the basis of the record, the FBI determined that there was reason to believe that this payment might have been for tickets for an unreported sidetrip across the border into the PRC to Beijing.
  11. Although Wen Ho Lee had visited IAPCM in both 1986 and 1988 and had filed “contact reports” claiming to recount all of the Chinese scientists he met there, he had failed to disclose his relationship with the PRC scientist who visited LANL in 1994.
  12. Wen Ho Lee worked on specialized computer codes at Los Alamos—so-called legacy codes related to nuclear testing data—that were a particular target for Chinese intelligence.
  13. The FBI learned that during a visit to Los Alamos by scientists from IAPCM, Lee had discussed certain unclassified hydrodynamic computer codes with the Chinese delegation. It was reported that Lee had helped the Chinese scientists with their codes by providing software and calculations relating to hydrodynamics.
  14. In 1997, Lee had requested permission to hire a graduate student, a Chinese national, to help him with work on “Lagrangian codes” at LANL. When the FBI evaluated this request, investigators were told by laboratory officials that there was no such thing as an unclassified Lagrangian code, which describes certain hydrodynamic processes and are used to model some aspects of nuclear weapons testing.
  15. In 1984, the FBI questioned Wen Ho Lee about his contact in 1982 with a US scientist at another DOE nuclear weapons laboratory who was under investigation.
  16. When questioned about this contact, Lee gave deceptive answers. After offering further explanations, Lee took a polygraph, claiming that he had been concerned only with this other scientist’s alleged passing of unclassified information to a foreign government against DOE and Nuclear Regulatory Commission regulations—something that Lee himself admitted doing. (As previously noted, the FBI closed this investigation of Lee in 1984.)
  17. The FBI, as noted above, had begun another investigation into Lee in the early 1990s, before the W-88 design information compromise came to light. This investigation was based upon an

---

FBI investigative lead that Lee had provided significant assistance to the PRC.

18. The FBI obtained a copy of a note on IAPCM letterhead dated 1987 listing three LANL reports by their laboratory publication number. On this note, in English, was a handwritten comment to “Linda” saying “[t]he Deputy Director of this Institute asked [for] these paper[s]. His name is Dr. Zheng Shaotang. Please check if they are unclassified and send to them. Thanks a lot. Sylvia Lee.”

The FBI request was worked into a draft FISA application by Mr. David Ryan, a line attorney from the Department of Justice’s Office of Intelligence Policy and Review (OIPR) with considerable experience in FISA matters. It was then reviewed by Mr. Allan Kornblum, as Deputy Counsel for Intelligence Operations, and finally, by Mr. Gerald Schroeder, Acting Counsel, OIPR.<sup>33</sup> As is well known by now, the OIPR did not agree to forward the FISA application, and yet another opportunity to discover what Dr. Lee was up to was lost.

The Department of Justice should have taken the FBI’s request for a FISA warrant on Dr. Lee to the court on 12 August 1997.

Attorney General Janet Reno testified about this case before the Senate Judiciary Committee on 8 June 1999. A redacted version of her testimony was released on 21 December 1999. The transcript makes it clear that the Department of Justice should have agreed to go forward with the search warrant for surveillance of Dr. Wen Ho Lee under the Foreign Intelligence Surveillance Act when the FBI made the request in 1997.

In evaluating the sufficiency of the FBI’s statement of probable cause, the Attorney General and the Department of Justice failed to follow the standards of the Supreme Court of the United States that the requirements for “domestic surveillance may be less precise than that directed against more conventional types of crime.” In *United States v. U.S. District Court* 407 U.S. 297, 322-23 (1972) the Court held:

*We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of “ordinary crime” . . . the focus of domestic surveillance may be less precise than that directed against more conventional types of crime . . . . Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection. [emphasis added]*

Even where domestic surveillance is not involved, the Supreme Court has held that the first focus is upon the governmental interest involved in determining whether constitutional standards are met. In *Camera v. Municipal Court of the City and County of San Francisco*, 387 U.S. 523, 534-539, (1967), the Supreme Court said:

*In cases in which the Fourth Amendment requires that a warrant to search be obtained, “probable cause” is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness. To apply this standard, it is obviously necessary first to focus upon the governmental interest which allegedly justifies official intrusion upon the constitutionally protected interests of the private citizen . . . [emphasis added]*

*Unfortunately, there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion, which the search entails . . . . The warrant procedure is designed to guarantee that a decision to search private property is justified by a reasonable governmental interest. But reasonableness is still the ultimate standard. If a valid public interest justifies the intrusion contemplated, then there is probable cause to issue a suitably restricted search warrant.*

Where the Court allowed inspections *in camera* without probable cause that a particular dwelling contained violations, it is obvious that even more latitude would be constitutionally permissible where national security is an issue, and millions of American lives may be at stake. Even under the erroneous, unduly high standard applied by the Department of Justice, however, the FBI's statement of probable cause was sufficient to activate the FISA warrant.

FBI Director Freeh correctly concluded that probable cause existed for the issuance of the FISA warrant. At the hearing on 8 June, Attorney General Reno stated her belief that there had not been a sufficient showing of probable cause but conceded that FBI Director Freeh, a former Federal judge, concluded that probable cause existed as a matter of law.<sup>34</sup>

The Department of Justice applied a clearly erroneous standard to determine whether probable cause existed. As noted in the transcript of Attorney General Reno's testimony:

*On 8-12-97 Mr. Allan Kornblum of OIPR advised that he could not send our (the FBI) application forward for those reasons. We had not shown that subjects were the ones who passed the W-88 [design information] to the PRC, and we had little to show that they were presently engaged in clandestine intelligence activities.*<sup>35</sup>

It is obviously not necessary to have a showing that the subjects were the ones who passed W-88 design information to the PRC. That would be the standard for establishing guilt at a trial, which is a far higher standard than establishing probable cause for the issuance of a search warrant. Attorney General Reno contended that other people, actually a relatively small number of people, would have to be ruled out as the ones who passed W-88 design information to the PRC before probable cause would be established for issuance of the FISA warrant on Dr. Lee. That, again, is the standard for conviction at trial instead of establishing probable cause for the issuance of a search warrant. For

some inexplicable reason, the Department of Justice has insisted on redacting the exact number of people who were situated similarly to Dr. Lee. However, it is apparent from the Kornblum statement that the wrong standard was applied, "that subjects were the ones that passed the W-88 [design information] to the PRC."<sup>36</sup>

DOJ was also wrong when Mr. Kornblum concluded that: "We had little to show that they were presently engaged in clandestine intelligence activities."<sup>37</sup> There is substantial evidence that Dr. Lee's relevant activities continued from the 1980s to 1992, 1994, and 1997 as noted above. When FBI Assistant Director John Lewis met with Attorney General Reno on 20 August 1997 to ask about the issuance of the FISA warrant, Attorney General Reno delegated the matter to Mr. Daniel Seikaly, former Director, DOJ Executive Office for National Security, and she had nothing more to do with the matter. Mr. Seikaly completed his review by late August or early September and communicated his results to the FBI through Mr. Kornblum. As Mr. Seikaly has testified, this was the first time he had ever worked on a FISA request, and he was not "a FISA expert." It was not surprising then that Seikaly applied the wrong standard for a FISA application:

*We can't do it (a FISA wiretap) unless there was probable cause to believe that that facility, their home, is being used or about to be used by them as agents of a foreign power.*<sup>38</sup>

Mr. Seikaly applied the standard from the typical criminal warrant as opposed to a FISA warrant. 18 U.S.C. 2518, governing criminal wiretaps, allows surveillance where there is:

*Probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted, are being used, or are about to be used in connection with the commission of such offense. [emphasis added]*

This criminal standard specifically requires that the facility be used in the "commission of such offense." FISA, however, contains no such

---

requirement, and 50 U.S.C. 1805 (Section 105 of FISA) states that a warrant shall be issued if there is probable cause to believe that:

*Each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.*

There is no requirement in this FISA language that the facility is being used in the commission of an offense.

Attorney General Reno demonstrated unfamiliarity with technical requirements of Section 1802 versus Section 1804. She was questioned about the higher standard under 1802 than 1804: “It seems the statutory scheme is a lot tougher on 1802 on its face.”<sup>39</sup>

Attorney General Reno replied, “Well I don’t know. I’ve got to make a finding that under 1804, that it satisfies the requirement and criteria—and requirement of such application as set forth in the chapter, and it’s fairly detailed.”<sup>40</sup>

When further questioned about her interpretation on 1802 and 1804, Attorney General Reno indicated a lack of familiarity with these provisions, saying:

*Since I did not address this, let me ask Ms. Townsend who heads the office of policy review to address it for you in this context and then I will . . .*<sup>41</sup>

As noted in the record, the offer to let Ms. Townsend answer the question was rejected in the interest of getting the Attorney General’s view on this important matter rather than that of a subordinate.

The lack of communication between the Attorney General and the Director of the FBI on a matter of such grave importance is troubling. As noted previously, Director Freeh sent John Lewis, Assistant FBI Director for National Security, to discuss this matter with the Attorney General on

20 August 1996. However, when the request for a review of the matter did not lead to the forwarding of the FISA application to the court, Director Freeh did not further press the issue. Attorney General Reno conceded that she did not follow up on the Wen Ho Lee matter. During the hearing on 8 June, Senator Sessions asked, “Did your staff convey to you that they had once again denied this matter?”<sup>42</sup>

Attorney General Reno replied, “No, they had not.”<sup>43</sup>

The hearing of 8 June 1999 also included a discussion as to whether FBI Director Freeh should have personally brought the matter again to Attorney General Reno. The Attorney General replied that she did not “complain” about FBI Director Freeh’s not doing so and stated, “I hold myself responsible for it.”<sup>44</sup> Attorney General Reno conceded the seriousness of the case, stating, “I don’t think the FBI had to convey to the attorneys the seriousness of it. I think anytime you are faced with facts like this it is extremely serious.”<sup>45</sup>

In the context of this serious case, it would have been expected that Attorney General Reno would have agreed with FBI Director Freeh that the FISA warrant should have been issued. In her testimony, she conceded that, if some 300 lives were at stake on a 747, she would take a chance, testifying, “My chance that I take if I illegally search somebody, if I save 300 lives on a 747, I’d take it.”<sup>46</sup>

In that context, with the potential for the PRC obtaining US secrets on nuclear warheads putting at risk millions of Americans, it would have been expected that the Attorney General would find a balance in favor of moving forward with the FISA warrant. As demonstrated by her testimony, Attorney General Reno sought, at every turn, to minimize the FBI’s statement of probable cause. On the issue of Dr. Lee’s opportunity to have visited Beijing while he was in Hong Kong and incurred additional travel costs of the approximate expense of traveling to Beijing, the Attorney General said that, “an unexplained travel voucher in Hong Kong does not lead me to the conclusion

---

that someone went to Beijing any more than they went to Taipei.”<sup>47</sup>

It might well be reasonable for a factfinder to conclude that Dr. Lee did not go to Beijing; but, certainly, his proximity to Beijing, the opportunity to visit there, and his inclination for having done so in the past would at least provide some “weight” in assessing probable cause. But the Attorney General dismissed those factors as having no weight even on the issue of probable cause, testifying, “I don’t find any weight when I don’t know where the person went.”<sup>48</sup> Of course, it is not known “where the person went.” If that fact had been established, it would have been beyond the realm of “probable cause.” Such summary dismissal by the Attorney General on a matter involving national security is inappropriate given the circumstances. In other legal contexts, opportunity and inclination are sufficient to cause an inference of certain conduct as a matter of law.

The importance of DOJ’s erroneous interpretation of the law in this case, which resulted in the FISA rejection, should not be underestimated. Had this application for a FISA warrant been submitted to the court, it doubtless would have been approved. DOJ officials reported that approximately 800 FISA warrants were issued each year with no one remembering any occasion when the court rejected an application.

Had the FBI obtained the FISA search warrant, it might have had a material effect on the investigation and criminal charging of Dr. Lee. Given the serious mistakes that had been made by the FBI prior to 1997, there is no guarantee that a FISA warrant would have led to a successful conclusion to the investigation, but the failure to issue a warrant clearly had an adverse impact on the case. Certainly, Dr. Lee would have been removed from a very sensitive job at least 18 months earlier, and the probabilities are high that significant additional incriminating evidence could have been found had Dr. Lee not had the opportunity to download the codes and conceal his taking of sensitive information.

To put the FISA rejection of 1997 in perspective, consider that the open network to which Dr. Lee had transferred the legacy codes was “linked to the Internet and e-mail, a system that had been attacked several times by hackers.”<sup>49</sup> Although we do not know the exact figures for the number of times that it was accessed, it has been reported that between October 1997 and June 1998 alone, “there were more than 300 foreign attacks on the Energy Department’s unclassified systems, where Mr. Lee had downloaded the secrets of the US nuclear arsenal.”<sup>50</sup>

Consider also the following from a government filing of 23 December 1999 in the criminal case against Dr. Lee:

*... in 1997 Lee downloaded directly from the classified system to a tenth portable computer tape a current nuclear weapons design code and its auxiliary libraries and utility codes.*<sup>51</sup>

This direct downloading had been made possible by Los Alamos computer managers who made Lee’s file transfers “easier in the mid-1990s by putting a tape drive on Lee’s classified computer.”<sup>52</sup> As incomprehensible as it seems, despite the fact that Dr. Lee was the prime suspect in an ongoing espionage investigation, and despite plans to restrict his access to classified information to limit any damage he might do, DOE computer personnel installed a tape drive on his computer that made it possible for him to directly download the nation’s top nuclear secrets. An important aim of surveillance under the FISA statute is to determine whether foreign intelligence services are getting access to our classified national security information. Despite what we know about Dr. Lee’s activities—and regardless of whether a jury ever finds that his acts were criminal—there should be no doubt that transferring classified information to an unclassified computer system and making unauthorized tape copies of that information created a substantial opportunity for foreign intelligence services to access that information.



---

## Investigation From 12 August 1997 to 23 December 1998

Notwithstanding the serious evidence against Dr. Lee on matters of great national security importance, the FBI investigation languished for 16 months—from August 1997 until December 1998—with the Department of Energy permitting Dr. Lee to continue on the job with access to classified information.

After OIPR's decision in August 1997 not to forward the FISA application, FBI Director Louis Freeh met with Deputy Energy Secretary Elizabeth Moler to tell her that there was no longer any investigatory reason to keep Lee in place at LANL and that DOE should feel free to remove him to protect against further disclosures of classified information. In October 1997, Director Freeh delivered the same message to Energy Secretary Federico Pena that he had given to Moler.<sup>53</sup> These warnings were not acted on, and Dr. Lee was left in place as were the files he had downloaded to the unclassified system, accessible to any hacker on the Internet.

After the rejection of the FISA warrant request on 12 August 1997, it took the FBI three and a half months to send a memo dated 19 December 1997 to the Albuquerque Field Office listing 15 investigative steps that should be taken to move the investigation forward. The Albuquerque Field Office did not respond directly until 10 November 1998. The 15 investigative steps were principally in response to the concerns raised by OIPR about the previous FISA request. To protect sources and methods, the specific investigative steps in the teletype of 19 December 1997 cannot be disclosed but have been summarized by the FBI as follows:

- Conduct additional interviews:
  - Open preliminary inquiries on other individuals named in the DOE AI who met critical criteria.
  - Develop information on associate's background and interview the associate.
  - Interview coworkers, supervisors, and neighbors.

- Conduct physical surveillance.
- Conduct other investigative techniques:
  - Review information resulting from other investigative methods.
  - Review other investigations for lead purposes.
  - Implement alternative investigative methods.<sup>54</sup>

As best as can be determined at this time, only two of the leads were seriously pursued. Most important, the FBI did not open investigations on the other individuals named in the DOE AI until recently.

The FBI conducted a false-flag operation against Dr. Lee in August 1998, in which an FBI agent posing as a Chinese intelligence officer contacted Lee. The FBI agent provided Dr. Lee with a beeper number and a hotel name. Dr. Lee did not immediately report this contact, but he told his wife who told a friend, who told DOE security. When Dr. Lee was questioned by DOE counterintelligence personnel about the phone call, he was vague and specifically failed to mention the beeper number or the hotel.

These additional steps did yield significant information that was relevant to supporting a determination of probable cause for a renewed FISA warrant, but the information was not used. While the FBI informally told OIPR of Dr. Lee's failure to fully report the August contact, that conversation did not take place until three months after the incident occurred.

The second lead that was pursued related to a potentially sophisticated communications system available to Dr. Lee, the specifics of which cannot be further detailed in this report for security reasons. This information, developed by the new agent in charge of the case and included in the 10 November 1998 FBI Albuquerque request for a new FISA application, would have been very important to OIPR's concerns about whether Dr. Lee was "currently engaged" in espionage, as well as the requirement for the activity to be clandestine.

---

Despite the development of significant relevant information on the probable cause issue, the FBI never made another formal request for DOJ to approve a new FISA warrant application after the OIPR decision in 1997 not to send the request forward. When such serious national interests were involved in this case, it was simply unacceptable for the FBI to tarry from 12 August 1997 to 19 December 1997 before sending the Albuquerque Field Office a memo. It was equally unacceptable for the Albuquerque field office to take from 19 December 1997 until 10 November 1998 to respond to the guidance from Headquarters, and then for the FBI not to renew the request for a FISA warrant based on the additional evidence.

### **DOE's Interference in the Investigation**

Dr. Lee traveled to Taiwan during the first three weeks of December 1998. The FBI agent who took over the case on 6 November 1998 did not agree with the DOE decision to have Wackenhut<sup>55</sup> give Dr. Lee a polygraph examination upon his return from Taiwan on 23 December 1998 and has called it "irresponsible." According to FBI protocol, Dr. Lee would have been questioned as part of a post-travel interview. However, the case agents were inexplicably unprepared to conduct such an interview. Ultimately, the polygraph decision was coordinated between DOE and the FBI's National Security Division. It should be noted, however, that the agent's concerns were supported by the report of June 1999 by the President's Foreign Intelligence Advisory Board, which recommended that the Attorney General determine, among other things, "why DOE, rather than the FBI, conducted the first polygraph in this case when the case was an open FBI investigation . . . ."<sup>56</sup>

There was no good reason for DOE to polygraph Dr. Lee in late 1998. There was no sudden change in status on the case: the last warning from the FBI about the need to remove Dr. Lee's classified access to protect national security had come some 14 months before, in October 1997. Available Department of Energy documents do not address this question. Other sources, including an FBI

HQ memorandum for Director Freeh, dated 21 December 1998, and a sworn deposition from an FBI agent who worked on the case, indicate that senior DOE officials were concerned about the imminent release of the *Cox Committee Report* and wanted to bring the case to a conclusion.

Even more important than the question of why DOE, rather than FBI, administered this polygraph is the way the results were reported. It should be noted that, as late as March 2000, there still exists considerable disagreement between the FBI and the DOE regarding the sequence and timing of events related to the production of information about the 23 December 1998 polygraph. When given an opportunity to contest the FBI's representation of the facts, DOE's Mr. Ed Curran said they were incorrect but was not prepared with specific contradictory information to offer as evidence. The resolution of these disagreements may ultimately turn on the credibility of the individuals involved in the disagreement and will be the subject of a future subcommittee hearing. According to the record as it now stands, the FBI was told on 23 December that Dr. Lee had passed the polygraph. The agents who were handling the case were given a summary sheet to support this conclusion but were not given access to the actual polygraph charts or the videotape of the interview.

Although DOE's quality-control review process apparently changed the interpretation of the polygraph results—concluding that Dr. Lee should be questioned again on key issues—that information was not immediately provided to the FBI. According to FBI records, the FBI's Albuquerque office did not receive the charts and videotapes from the 23 December polygraph until 22 January 1999. When FBI polygraph experts in early February subsequently analyzed the charts and videotape, they concluded that Dr. Lee had failed relevant questions<sup>57</sup> or was, at best, inconclusive.<sup>58</sup> Based on these concerns, the FBI arranged for additional interviews and a new polygraph on 10 February 1999.

The DOE failed to keep the FBI fully informed on the polygraph issue in a timely fashion. Although they were present at the exam, FBI agents did not

---

receive the polygraph charts until a month later, even though Wackenhut quality-control personnel had assessed the charts on 23 December and again on 28 December. No satisfactory explanation has yet been offered for this delay. It should be noted, however, that according to an FBI memorandum of 26 February 1999, DOE employees were initially instructed not to provide the FBI with the full results of the polygraph, only the summary sheet.

On this state of the record, it appears that DOE did take the position that Dr. Lee passed the 23 December polygraph. As late as 16 March 1999, Energy Secretary William Richardson said on *CNN Crossfire* that DOE “instituted a polygraph on this person, which he first passed.”<sup>59</sup> Secretary Richardson then described a second polygraph, apparently referring to the FBI-administered polygraph in February, which Dr. Lee failed.

Given the representation by DOE that Dr. Lee passed the polygraph, it is not surprising that the FBI’s investigation of Dr. Lee was thrown off course in late 1998. In contrast with the FBI’s renewed efforts for the FISA warrant—as laid out in the teletype of 10 November 1998 from the Albuquerque office—when told by DOE that Dr. Lee had passed the polygraph, the FBI interviewed him on 17 January 1999,<sup>60</sup> and in a teletype dated 22 January 1999 to FBI HQ, in effect, concluded that the investigation should not be pursued.

In late January 1999, Dr. Lee began erasing the classified files from the unsecured area of the computer. After the interview on 17 January, Dr. Lee “began a sequence of massive file deletions . . .”<sup>61</sup> He even called the help desk at the Los Alamos computer center to get instructions for deleting files. After he was interviewed and polygraphed again on 10 February within two hours of the time he was told he had failed the exam, he deleted even more files. All told, Dr. Lee deleted files on 20 January and 9, 10, 11, 12, and 17 February. When he called the help desk on 22 January, his question indicated that he did not know that the “delay” function of the computer he was using would keep deleted files in the directory for some period of time. He asked why, when he deleted

files, were the ones in parentheses not going away, and asked how to make them go away immediately. On 16 February, he also asked how to replace an entire file on a tape.<sup>62</sup>

Thus, the report that Dr. Lee had passed the polygraph of 23 December 1998 gave him precious time to delete and secrete information. The significance of Dr. Lee’s file deletions—and the unreasonable delays in carrying out the investigation that should have detected and prevented them—should not be underestimated. As FBI Agent Robert Messemer has testified, the FBI came very close, “within literally days, of having lost that material.”<sup>63</sup> The FBI was almost unable to prove that Dr. Lee downloaded classified files. If the material had been overwritten after it was deleted, “that deletion by Dr. Lee [would] have kept that forever from this investigation.” In this context, the repeated delays and the lack of coordination between the FBI and the Department of Energy—and later between the FBI and the Department of Justice—are much more serious.

## 10 February 1999 to 8 March 1999

On 10 February 1999, Wen Ho Lee was again given a polygraph examination, this time by the FBI. During this second test, which Lee failed, he was asked: “Have you ever given any of [a particular type of classified computer code related to nuclear weapons testing] to any unauthorized person?” and “Have you ever passed W-88 information to any unauthorized person?”<sup>64</sup> It should be noted that the 1997 FISA request mentioned that the PRC was using certain computational codes, which were later identified as something to which Lee had unique access.<sup>65</sup> Moreover, the computer code information had been developed independently of the DOE Administrative Inquiry, which is now being questioned by FBI and DOJ officials.

After this second failed polygraph, there should have been no doubt that Dr. Lee was aware he was a suspect in an espionage investigation, and it is inconceivable that neither the FBI nor DOE personnel took the rudimentary steps of checking

---

to see if he was engaging in any unusual computer activity. Again, this is not hindsight. The classified information to which Dr. Lee had access, and which he had been asked about in the polygraph, was located on the Los Alamos computer system. The failure of DOE and FBI officials to promptly find out what was happening with Dr. Lee's computer after he was deceptive on the code-related polygraph question is inexplicable. As noted above, this failure afforded Dr. Lee yet another opportunity to erase files from both the unsecured system and the unauthorized tapes he had made.

As should have been expected, Dr. Lee used the time afforded him by the delays to delete the classified information he had placed on the unclassified system. He also approached two other T-Division employees with a request to use their tape drive to delete classified data from two tapes (he no longer had access to the one that had been installed in his X-Division computer since he had been moved from that division in December 1998).

Nearly three weeks after the polygraph failure, the FBI finally asked for and received permission to search Lee's office and his office computer, whereupon they began to discover evidence of his unauthorized and unlawful computer activities. Even so, the FBI did not immediately move to request a search warrant. The three-week delay, from 10 February until the first week of March, is inexplicable.

### **8 March 1999 to 7 April 1999**

Dr. Lee was fired on 8 March 1999. While it is difficult to understand why the FBI did not move more quickly after the February polygraph failure, the subsequent delay—from when Wen Ho Lee was fired on March 8, until a search warrant for his home was finally obtained on April 9—is equally inexplicable. Rather than moving quickly to discover the extent of the potential damage, FBI and DOJ officials continued to wrangle over whether the matter should be handled under FISA or was “way too criminal” for that.<sup>66</sup> Meanwhile, information that could change the global strategic

balance was left exposed on an unclassified computer system where even an unsophisticated hacker could gain access to it.

It was not until nearly a month after Lee was fired that progress was made on the search warrant issue. Only after a meeting on 7 April 1999, when FBI officials indicated that FBI Director Freeh was “prepared formally to supply the necessary certifications that this search met the requirements of the FISA statute—that is, that it was being sought for purposes of intelligence collection (*e.g.*, to learn about Lee's alleged contacts with Chinese intelligence),”<sup>67</sup> did the search warrant process begin to move forward.

At this 7 April meeting, OIPR attorneys raised their old concerns about the currency and sufficiency of the evidence against Lee, as well as new concerns about the appearance of improperly using FISA for criminal purposes and the prospect of conducting an unprecedented overt FISA search.<sup>68</sup> Frustrated that the Criminal Division continued to believe that the FBI's draft affidavit contained an insufficient showing of probable cause to search Lee's residence, FBI officials began working with an Assistant US Attorney in Albuquerque to craft a second affidavit that was presented to a US Magistrate Judge on 9 April 1999 and was executed without incident the following day.<sup>69</sup>

### **Reopening the W-88 Investigation and the Criminal Case Against Dr. Lee**

The decision in September 1999 by the FBI and the DOJ to expand the investigation of suspected Chinese nuclear espionage<sup>70</sup> is puzzling, primarily because it should have happened long ago. Assistant FBI Director Neil Gallagher's letter of 10 November 1999 on the question of why the investigation is being reopened raises more questions than it answers. He acknowledges that, when discussing the DOE's AI during his 9 June 1999 testimony before the Governmental Affairs Committee,<sup>71</sup> he stated that, he “had full credibility in the report,” had “found nothing in DOE's AI, nor the conclusions drawn from it to be erroneous,” and



---

stated there is a “compelling case made in the AI to warrant focusing on Los Alamos.”<sup>72</sup>

As a result of further inquiry, however, Mr. Gallagher now has reason to question the conclusions of the AI. He cites an interview on 20 August 1999 by FBI officials of one of the scientists who participated in the technical portion of the AI, in which the scientist “stated that he had expressed a dissenting opinion with respect to the technical aspects of the AI,” and points out that the statement of this scientist is “in direct conflict with the AI submitted to the FBI because the AI does not reflect any dissension by the ‘DOE Nuclear Weapons Experts.’”<sup>73</sup>

Although both the FBI and the DOE have repeatedly promised to do so, neither agency has yet provided an answer as to how many scientists were involved in the technical review mentioned in the interview of August 1999 and what the majority opinion of that group really was. Mr. Gallagher explains that “a review has been initiated by the FBI to re-evaluate the scope of the AI,” and that, “the focus of this new initiative is to determine the full universe of both compromised restricted nuclear weapons information and who had access to that information in addition to anyone identified in the original AI.”<sup>74</sup>

The delay by DOJ and the FBI until September 1999 is perplexing since four governmental reports had concluded—with varying degrees of specificity—that the losses of classified information extended beyond W-88 design information and beyond Los Alamos:

- The classified version of the *Cox Committee Report* (January 1999).
- The damage assessment of 21 April 1999 by Mr. Robert Walpole, the National Intelligence Officer for Strategic and Nuclear Programs.<sup>75</sup>
- The unclassified version of the *Cox Committee Report* (May 25, 1999).
- The *Special Report of the President’s Foreign Intelligence Advisory Board* (June 1999).

All of these reports gave FBI and DOJ ample evidence that further investigation was necessary. For example, the *Cox Committee Report* states flatly, “the PRC stole classified information on every currently deployed US inter-continental ballistic missile (ICBM) and submarine-launched ballistic missile (SLBM).”<sup>76</sup> Tellingly, the Cox Committee notes that, “a Department of Energy investigation of the loss of technical information about the other five US thermonuclear warheads had not begun as of January 3, 1999 . . .” and that, “the FBI had not yet initiated an investigation” as of that date.<sup>77</sup> Thus, the failure to reopen the investigation into the loss of W-88 design information much sooner, or to even initiate an investigation of the other losses, simply continued that pattern of errors.

The subcommittee’s investigation thus far has identified several areas where reform is necessary and identified appropriate solutions. These solutions have been incorporated in the “Counter-Intelligence Reform Act of 2000,” which is summarized below:

1. This bill amends the Foreign Intelligence Surveillance Act by providing that, upon the personal request of the Director of the FBI, the Secretary of State, the Secretary of Defense, or the Director of Central Intelligence, the Attorney General shall personally review a FISA application. The failure to forward the FISA request to the court in 1997 represents a critical failure in this case. When the “global strategic balance” is an issue, the Attorney General should not delegate the review to subordinates with no experience in FISA matters, as happened in this instance. Because this provision is triggered only by a personal request from the Director of the FBI or one of the other few Cabinet officials authorized to request FISA warrants, it will not impose upon the duties of the Attorney General except in truly exceptional cases where such imposition is clearly warranted.
2. If the Attorney General decides not to forward the application for a warrant to the



---

court, that decision must be communicated in writing to the requesting official with specific recommendations on what additional investigation should be undertaken to establish the requisite probable cause. A decision to reject a FISA application should come only after careful analysis of the specifics. Should the Attorney General still decline to go forward with a request after such analysis, the requesting agency should have the benefit of that analysis, as well as a plan to remedy any deficiencies. By definition, this section will apply only in cases where the Director of the FBI or another senior Cabinet official has made a personal appeal to the Attorney General. By communicating the reasons for the rejection in writing, along with recommendations for improvements, the Attorney General can facilitate the proper functioning of the FISA process to ensure that the national security is not put at risk due to misunderstandings about the showing of probable cause in a case.

3. The requesting official must personally supervise the implementation of the Attorney General's recommendations. The FBI's delay of three and a half months after the decision in August 1997 regarding the FISA application and the delay from 19 December 1997 until 10 November 1998 for a response by the Albuquerque office was unacceptable in the context of the national security information at risk. In cases of such great importance, the personal knowledge and supervision by top officials is appropriate and necessary.
4. This bill addresses the issue of whether an individual is "presently engaged" in the particular activity in order not to preclude conduct in the past from serving as the basis for a warrant—even if a substantial period of time has elapsed—recognizing that espionage or related activities usually span a considerable period of time, causing the legislature to omit any statute of limitations for such crimes. Where directly relevant conduct has occurred in the past, it should not be excluded if it reasonably can be interpreted as indicating that

an individual is involved in espionage. OIPR's focus on the contention that the W-88 information had been lost some ten years earlier was clearly misplaced. The loss of our national security information is so important that it must be investigated, even if discovered somewhat after the fact. Keeping in mind that FISA surveillance is primarily for intelligence rather than for criminal purposes, such events should not be unnecessarily excluded from consideration.

5. Finally, this bill improves the coordination of counterintelligence activities by requiring that:
  - a. If the FBI requests a FISA warrant on an individual with whom it or any law enforcement or intelligence agency has a relationship, that fact must be disclosed to OIPR as part of the FISA request.
  - b. When the FBI desires to leave an individual in place for investigative reasons, that decision must be communicated in writing to the head of the affected agency, along with a plan to minimize the potential for harm to the national security, which shall take precedence over investigative concerns. The agency head must, likewise, respond in writing, and any disagreements over the proper course of action will be referred to the National Counterintelligence Policy Board.
  - c. When the FBI opens a counterintelligence investigation on a subject, it must coordinate with other intelligence and law enforcement agencies to identify any relationship between the subject and those entities.

I urge prompt consideration of these proposals.

---

## Endnotes

<sup>1</sup> Stephen Younger, "Transcript of Proceedings, Detention Hearing in the case of United States vs. Wen Ho Lee," 13 December 1999: 38 (hereafter referred to as Transcript of Proceedings).

<sup>2</sup> Transcript of Proceedings, 38.

<sup>3</sup> Transcript of Proceedings, Motion Hearing, 27 December 1999: 4. (hereafter referred to as Motion Hearing).

<sup>4</sup> This information was drawn from Dr. Lee's Web site at <http://wenholee.org/whois.htm>.

<sup>5</sup> United States of America, "Response to Defendant Wen Ho Lee's Motion to Revoke Judge's Svet's Order of Detention," 23 December 1999: 10. See also, United States Senate, Selection Committee on the Judiciary, Redacted Transcript of Closed Hearing with Attorney General Janet Reno Regarding the FISA Process in the Wen Ho Lee Case, 8 June 1999: 14-16.

<sup>6</sup> Ibid. 10. See also, United States Senate, Select Committee on the Judiciary, Redacted Transcript of Closed Hearing with Attorney General Janet Reno Regarding the FISA Process in the Wen Ho Lee Case, 8 June 1999: 15 (hereafter referred to as Redacted Transcript).

<sup>7</sup> Redacted Transcript, 15.

<sup>8</sup> Redacted Transcript, 15.

<sup>9</sup> "Response to Defendant Wen Ho Lee's Motion to Revoke Judge Svet's Order of Detention," 23 December 1999: 13, footnote 4.

<sup>10</sup> Ian Hoffman, "Agent: Lee Admitted Lying," *Albuquerque Journal*, 18 January 2000, online edition.

<sup>11</sup> Redacted Transcript, 16.

<sup>12</sup> Redacted Transcript, 16-17; Senators Thompson and Lieberman's statement, 6, 16.

<sup>13</sup> James Risen and David Johnston, "U.S. Will Broaden Investigation of China Nuclear Secrets Case," *New York Times*, 23 September 1999, online edition. Notes. 55.

<sup>14</sup> Senators Thompson and Lieberman's statement, 6, footnote 14.

<sup>15</sup> Redacted Transcript, 108-109.

<sup>16</sup> Redacted Transcript, 109.

<sup>17</sup> Redacted Transcript, 109.

<sup>18</sup> Ian Hoffman, "Lawyer: Lee's Intent in Question," *Albuquerque Journal*, 5 January 2000 at <http://wenholee.org/ABQJournal010500.htm>.

<sup>19</sup> For a discussion of this issue, see Motion Hearing, 147-157.

<sup>20</sup> Motion Hearing, 152-153.

<sup>21</sup> United States of America, "Response to Defendant Wen Ho Lee's Motion to Revoke Judge Svet's Order of

Detention," 23 December 1999.

<sup>22</sup> William Broad, "Spies Versus Sweat: The Debate Over China's Nuclear Advance," *New York Times*, 7 September 1999, online edition.

<sup>23</sup> Vernon Loeb and Walter Pincus, "China Prefers the Sand to the Moles," *Washington Post*, 12 December 1999, A02.

<sup>24</sup> United States House of Representatives, *Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China*, 25 May 1999: Volume 1, 83-84 (hereafter referred to as *Cox Report*). A "walk-in" is an individual who voluntarily offers to conduct espionage.

<sup>25</sup> President's Foreign Intelligence Advisory Board, *Science at its Best; Security at its Worst*, June 1999, 30-31 (hereafter referred to as PFIAB).

<sup>26</sup> Senators Thompson and Lieberman's statement, 6-7.

<sup>27</sup> X-Division Open Lan Rules of Use, executed by Dr. Wen Ho Lee on April 19, 1995.

<sup>28</sup> Senators Thompson and Lieberman's statement, 9.

<sup>29</sup> "Richardson Announces Results of Inquiries Related to Espionage Investigation," Department of Energy News Release, 12 August 1999.

<sup>30</sup> Senators Thompson and Lieberman's statement, 9.

<sup>31</sup> This list has been extracted from the 5 August 1999, Statement by Senate Governmental Affairs Committee Chairman Fred Thompson and Ranking Minority Member Joseph Lieberman, *Department of Energy, FBI, and Department of Justice Handling of Espionage Investigation into the Compromise of Design Information on the W-88 Warhead*, 14-17.

<sup>32</sup> Hydrodynamics is a science that is relevant to the development of nuclear weapons design.

<sup>33</sup> Redacted Transcript, 35 and 88.

<sup>34</sup> Redacted Transcript, 118-119.

<sup>35</sup> Redacted Transcript, 52. In a 6 March 2000 letter from Assistant Attorney General Robert Rabin to Senator Hatch, the Department of Justice takes issue with this statement and quotes Senator Kyl's testimony on the subject, "So it would be your view that (the language quoted in the draft report) is a summary that probably overstates the Justice Department's requirements for the FBI? The Attorney General responded, "That is correct." Transcript of 8 June 1999 at 49." (sic) For the actual exchange, see page 53 of the 8 June 1999 transcript.

<sup>36</sup> Redacted Transcript, 52.

<sup>37</sup> Redacted Transcript, 52.

<sup>38</sup> Unclassified excerpt of Mr. Seikaly's testimony before the Senate Select Committee on Intelligence, May 1999.

<sup>39</sup> Redacted Transcript, 49.

---

<sup>40</sup> Redacted Transcript, 49.  
<sup>41</sup> Redacted Transcript, 24-25.  
<sup>42</sup> Redacted Transcript, 39.  
<sup>43</sup> Redacted Transcript, 39..57.  
<sup>44</sup> Redacted Transcript, 40.  
<sup>45</sup> Redacted Transcript, 36.  
<sup>46</sup> Redacted Transcript, 56.  
<sup>47</sup> Redacted Transcript, 117.  
<sup>48</sup> Redacted Transcript, 117.  
<sup>49</sup> Motion Hearing, 85. See also Pete Carey, "Los Alamos Suspect May Have Been Doing His Job: Rerouting Files Common at Lab," *Florida Times-Union*, 20 June 1999, G-8.  
<sup>50</sup> "With Intent to Injure the U.S.," *Washington Times* editorial, 14 December 1999, A16.  
<sup>51</sup> United States of America, "Response to Defendant Wen Ho Lee's Motion to Revoke Judge Svet's Order of Detention," December 23, 1999, 3-4.  
<sup>52</sup> Ian Hoffman.  
<sup>53</sup> Senators Thompson and Lieberman's statement, 23-24.  
<sup>54</sup> Unclassified summary of the 19 December 1997, FBIHQ teletype to Albuquerque, provided by FBI Office of Public and Congressional Affairs, 3 December 1999.  
<sup>55</sup> Wackenhut is a private company that has a contract with DOE to perform security-related polygraphs.  
<sup>56</sup> PFIAB, 34.  
<sup>57</sup> See FBI Headquarters internal memo dated 2 February 1999 and/or 6 February 1999 on the same subject.  
<sup>58</sup> United States Senate, Committee on Governmental Affairs, testimony from 9 June 1999 closed hearing: 145.  
<sup>59</sup> The information regarding Secretary Richardson's public statements on the polygraph question can be found in footnote 108 of the 5 August 1999, special statement of the Senate Governmental Affairs Committee. 58.  
<sup>60</sup> Transcript of Proceeding, Detention Hearing, in the case of U.S. v. Wen Ho Lee, December 13, 1999, before the Honorable Don J. Svet in the U.S. District Court for the District of New Mexico: 118.  
<sup>61</sup> Transcript of Proceeding, 118.  
<sup>62</sup> For a detailed discussion of Dr. Lee's deletions and his call to the computer help line, see "Transcript of Proceedings, Motion Hearing, December 27, 1999," *United States of America vs. Wen Ho Lee*, pages 132-138.  
<sup>63</sup> Transcript of Proceedings, 146.  
<sup>64</sup> Senators Thompson and Lieberman's Statement, 26.  
<sup>65</sup> For a detailed discussion of the computer code issue, see the transcript of Attorney General Reno's testimony

before the Senate Judiciary Committee on 8 June 1999, 108-109 (as numbered in the lower right-hand corner).

<sup>66</sup> For a discussion of the debate between FBI and DOE after Lee's computer was searched, see Senators Thompson and Lieberman's statement, 27-29.  
<sup>67</sup> Senators Thompson and Lieberman's statement, 28.  
<sup>68</sup> Senators Thompson and Lieberman's statement, 28-29.  
<sup>69</sup> Senators Thompson and Lieberman's statement, 27-28. In a 6 March 2000 letter to Senator Hatch, Assistant Attorney General Robert Rabin expressed the views of the Department of Justice on the subpoena issue, " . . . the Department disagrees with the draft's characterization of the role the Criminal Division played in obtaining a search warrant for Mr. Lee's residence. The Criminal Division in Washington and the US Attorney's Office in Albuquerque worked together throughout the process of obtaining a search warrant for Wen Ho Lee's home. After discussing the issue together, both offices agreed that the first draft search warrant affidavit needed additional facts to establish probable cause. That conclusion was communicated in a joint conference call of both Offices with the FBI. The revised affidavit submitted by the FBI was reviewed and approved by both Offices working together, and was then presented to the US Magistrate Judge on 9 April 1999.

<sup>70</sup> For example, see the 28 September 1999 press release from the FBI National Press Office, which states that Special Agent in Charge Steve Dillard "has been appointed as Inspector in Charge of a task force composed of FBI Special Agents and analysts that will investigate the possible theft or compromise of classified information from United States nuclear laboratories . . . ." The full text of the press release is available at <http://www.fbi.gov/pressrm/pressrel/dillard.htm>.

<sup>71</sup> He made similar representations in other briefings provided to Senate staff.

<sup>72</sup> Gallagher, letter of 10 November 1999, 1.

<sup>73</sup> Gallagher, letter of 10 November 1999, 2.

<sup>74</sup> Gallagher, letter of 10 November 1999, 2-3.

<sup>75</sup> See "DCI Statement on Damage Assessment," at [http://www.cia.gov/cia/public\\_affairs/press\\_release/ps042199.html](http://www.cia.gov/cia/public_affairs/press_release/ps042199.html), and the "Key Findings" at [http://www.cia.gov/cia/public\\_affairs/press\\_release/0421kf.html](http://www.cia.gov/cia/public_affairs/press_release/0421kf.html).

<sup>76</sup> *Cox Committee Report*, Vol. 1, 68.

<sup>77</sup> *Cox Committee Report*, Vol. 1, 83-84

---

**David Tzu Wvi Yang and Eugene You Tsai Hsu**

On 30 August 2001, US Customs arrested David Tzu Wvi Yang and Eugene You Tsai Hsu for attempting to export military encryption technology to China in violation of the Arms Control Export Act.

According to an affidavit filed in federal court, Hsu—of Blue Springs, Missouri—and Yang—of Temple City, California—were attempting to export to China encryption devices used to secure and safeguard classified communications. Hsu was arrested at his home in Blue Springs, Missouri. Yang was arrested at his place of business in Compton, California.

The KIV-7HS encryption unit/technology is designed for government use only and cannot be legally exported from the United States without first obtaining an export license from the State Department. China, however, is prohibited from acquiring KIV-7HS unit/technology from the United States.

In May 2001, Hsu contacted Mykotronx, Inc., a private company located in Columbia, Maryland, to inquire about the cost of the KIV-7HS unit/technology. A security officer at Mykotronx subsequently contacted US Customs agents in Baltimore to alert them to Hsu's interest in obtaining the technology. US Customs agents instructed Mykotronx to inform Hsu that all future inquiries relative to the KIV-7HS units would be handled through an intermediary import/export entity located in Maryland.

During the period 2 May to 18 August 2001, an undercover Customs agent, posing as the intermediary, engaged in a series of telephone conversations and faxed correspondence with Hsu, Charlson Ho, and David Yang. The telephone conversations and correspondence revealed that Ho, affiliated with Wei Soon Loong Private, LTD., a Singapore-based company, was the buyer of the KIV-7HS units.

Ho disclosed to the Customs undercover agent that his freight forwarder, David Yang, would handle the export of the KIV-7HS units through his business in Compton, California—Dyna Freight. A check of Immigration and Naturalization Service (INS) records indicated that Yang was born in Taiwan and is a permanent resident alien of the United States.

The undercover Customs agent advised Hsu that the KIV-7HS units are Munitions List items and would require a license for export. Hsu asked if the undercover agent could obtain the license. After being told by the undercover agent that no license would be approved for export to China and that export to China would be a violation of the Arms Control Export Act, Hsu continued to show interest. A check of INS records confirmed that Hsu is a naturalized US citizen.

On 24 August 2001, Yang confirmed to the Customs undercover agent that the KIV-7HS units would be shipped from Los Angeles through Taipei to Singapore, where Ho would then forward the units to China.

---

**PUBLIC ANNOUNCEMENT****U.S. DEPARTMENT OF STATE  
Office of the Spokesman****CHINA  
April 19, 2001**

The Ministry of State Security (MSS) of the People's Republic of China has recently taken into custody several American citizens and U.S. permanent residents of Chinese origin. Of these, at least two Americans are now being detained by the Chinese authorities under suspicion of espionage or damaging China's national security, even though the Chinese Government has not offered any evidence to substantiate these allegations. Others have been questioned for up to four days and then released.

The Department of State cautions Americans, especially Americans originally from China, that there may be a risk of being detained upon returning to China, if they have at any time engaged in activities or published writings critical of Chinese government policies. In some cases, travel to Taiwan or involvement with Taiwan media organizations has apparently also been regarded as the equivalent of espionage by MSS. Therefore, persons with a history of such activities or writings should carefully evaluate this information in deciding whether to travel to China.

It should be noted as well that the Americans recently detained by MSS had previously visited China without incident, but were nonetheless detained during their most recent visits. At least two of the Americans were identified by MSS as persons of interest, even though they had changed their names in the U.S. upon naturalization or marriage.